TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

AVIS INFORMANT LE DEPOSANT DE LA COMMUNICATION DE LA DEMANDE INTERNATIONALE AUX OFFICES DESIGNES

(règle 47.1.c), première phrase, du PCT)

Destinataire:
CORLU, Bernard
Bull S.A.
PC58D20
68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

Direction de la Propriété Intellectuelle
29 AOUT 2000
BULL S.A.

Date d'expédition (jour/mois/année) 17 août 2000 (17.08.00)	
Référence du dossier du déposant ou du mandataire PCT 3775/BC	**AVIS IMPORTANT**

Demande internationale no	**Date du dépôt international** (jour/mois/année)	**Date de priorité** (jour/mois/année)
PCT/FR00/00332	10 février 2000 (10.02.00)	11 février 1999 (11.02.99)

Déposant
BULL S.A. etc

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:
   US

   Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:
   CA,EP,JP

   La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1)a-bis)).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau international le
   17 août 2000 (17.08.00) sous le numéro WO 00/48355

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, **la demande d'examen préliminaire international** doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le volume II du Guide du déposant du PCT.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé
J. Zahra

no de téléphone (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
PCT 3775/BC		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 00/00332	10/02/2000	11/02/1999
Déposant		
BULL S.A. et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 5 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [X] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant

   [ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° 2a

   [X] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n° PCT/FR 00/00332

Cadre I Observations – lorsqu'il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (suite du point 1 de la première feuille)

Conformément à l'article 17.2)a), certaines revendications n'ont pas fait l'objet d'une recherche pour les motifs suivants:

1. ☐ Les revendications n^{os} se rapportent à un objet à l'égard duquel l'administration n'est pas tenue de procéder à la recherche, à savoir:

2. ☐ Les revendications n^{os} se rapportent à des parties de la demande internationale qui ne remplissent pas suffisamment les conditions prescrites pour qu'une recherche significative puisse être effectuée, en particulier:

3. ☐ Les revendications n^{os} sont des revendications dépendantes et ne sont pas rédigées conformément aux dispositions de la deuxième et de la troisième phrases de la règle 6.4.a).

Cadre II Observations – lorsqu'il y a absence d'unité de l'invention (suite du point 2 de la première feuille)

L'administration chargée de la recherche internationale a trouvé plusieurs inventions dans la demande internationale, à savoir:

voir feuille supplémentaire

1. ☒ Comme toutes les taxes additionnelles ont été payées dans les délais par le déposant, le présent rapport de recherche internationale porte sur toutes les revendications pouvant faire l'objet d'une recherche.

2. ☐ Comme toutes les recherches portant sur les revendications qui s'y prêtaient ont pu être effectuées sans effort particulier justifiant une taxe additionnelle, l'administration n'a sollicité le paiement d'aucune taxe de cette nature.

3. ☐ Comme une partie seulement des taxes additionnelles demandées a été payée dans les délais par le déposant, le présent rapport de recherche internationale ne porte que sur les revendications pour lesquelles les taxes ont été payées, à savoir les revendications n^{os}

4. ☐ Aucune taxe additionnelle demandée n'a été payée dans les délais par le déposant. En conséquence, le présent rapport de recherche internationale ne porte que sur l'invention mentionnée en premier lieu dans les revendications; elle est couverte par les revendications n^{os}

Remarque quant à la réserve

☐ Les taxes additionnelles étaient accompagnées d'une réserve de la part du déposant.

☒ Le paiement des taxes additionnelles n'était assorti d'aucune réserve.

SUITE DES RENSEIGNEMENTS INDIQUES SUR PCT/ISA/ 210

L'administration chargée de la recherche internationale a trouvé plusieurs (groupes d') inventions dans la demande internationale, à savoir:

1. revendications: 1-5

   Procédé de vérification de l'usage de clés publiques

2. revendication : 6

   Système comprenant des moyens pour faire une demande de certification, de telle façon que l'origine de la requête puisse être vérifiée

RAPPORT DE RECHERCHE INTERNATIONALE

[redacted] de Internationale No
[redacted] FR 00/00332

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/08 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	HOLLOWAY C: "Controlling the use of cryptographic keys" PROCEEDINGS OF COMPSEC INTERNATIONAL 1995, PROCEEDINGS OF COMPSEC INTERNATIONAL 95. TWELFTH WORLD CONFERENCE ON COMPUTER SECURITY, AUDIT AND CONTROL, LONDON, UK, 25-27 OCT. 1995, pages 587-598, XP000584311 Oxford, UK, Elsevier, UK ISBN: 1-85617-294-5 page 590, colonne 1, dernier alinéa -page 597 --- -/--	1-5

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
16 août 2000	28. 08. 2000
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fonctionnaire autorisé Zucka, G

3

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	MATYAS S M: "Key handling with control vectors" IBM SYSTEMS JOURNAL, 1991, USA, vol. 30, no. 2, pages 151-174, XP000234622 ISSN: 0018-8670 page 162 -page 163 page 169 ---	1
A	EP 0 576 224 A (NCR INT INC) 29 décembre 1993 (1993-12-29) colonne 3, ligne 30 -colonne 10, ligne 12 ---	1
A	EP 0 456 553 A (BULL SA) 13 novembre 1991 (1991-11-13) colonne 7, ligne 15 -colonne 15, ligne 12 ---	1-6
A	EP 0 539 726 A (IBM) 5 mai 1993 (1993-05-05) colonne 11, ligne 48 -colonne 12, ligne 1 -----	1-6

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No [redacted]/FR 00/00332

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0576224 A	29-12-1993	DE 69307198 D	20-02-1997
		DE 69307198 T	18-09-1997
		JP 6069915 A	11-03-1994
		US 5555309 A	10-09-1996
EP 0456553 A	13-11-1991	FR 2662007 A	15-11-1991
		CA 2041761 C	11-04-1995
		DE 69101257 D	07-04-1994
		DE 69101257 T	07-07-1994
		US 5214700 A	25-05-1993
EP 0539726 A	05-05-1993	US 5164988 A	17-11-1992
		CA 2071413 A,C	01-05-1993
		DE 69230489 D	03-02-2000
		DE 69230489 T	15-06-2000
		JP 2552061 B	06-11-1996
		JP 5216411 A	27-08-1993

PCT

ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L 9/00

A2

(11) Numéro de publication internationale: WO 00/48355

(43) Date de publication internationale: 17 août 2000 (17.08.00)

(21) Numéro de la demande internationale: PCT/FR00/00332

(22) Date de dépôt international: 10 février 2000 (10.02.00)

(30) Données relatives à la priorité:
99/01652 11 février 1999 (11.02.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: BULL S.A. [FR/FR]; 68, route de Versailles, F–78434 Louveciennes Cedex (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(US seulement)*: PINKAS, Denis [FR/FR]; 13 Pavé des Gardes, F–92370 Chaville (FR).

(74) Mandataire: CORLU, Bernard; Bull S.A., PC58D20, 68, route de Versailles, F–78434 Louveciennes Cedex (FR).

(81) Etats désignés: CA, JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

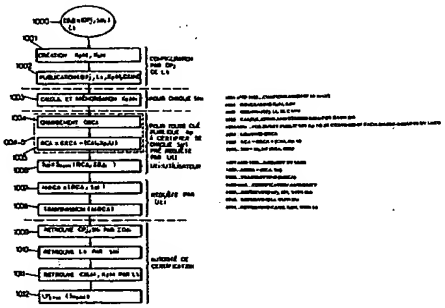
Publiée

Sans rapport de recherche internationale, sera republiée dès réception de ce rapport.

(54) Title: METHOD FOR VERIFYING THE USE OF PUBLIC KEYS GENERATED BY AN ON–BOARD SYSTEM

(54) Titre: PROCEDE DE VERIFICATION DE L'USAGE DE CLES PUBLIQUES ENGENDREES PAR UN SYSTEME EMBARQUE

(57) Abstract



The invention concerns an on–board system for verifying a certification request of a public key (K_p) generated by an on–board identifier system (SN_i). For an assembly (Lk) of on–board systems, an authorised identifier (OP_j) operator configures the on–board systems and generates (1001) a parent public key (KpM) and a parent private key (KsM). The identifier (Op_j), the reference range of identifiers (Lk) and the public key (KpM) are issued (1002). For each on–board system (SN_i), a diversified key (KsM_i) is generated from the identifier (SN_i) and stored (1003) in a storage unit with protected reading and writing access. For every public key (Kp) generated by an on–board system, a cryptographic control value (Sci) is computed (1006) on the public key (Kp), an algorithm identifier (CA1) and utilisation parameters (U) of said key using a zero–knowledge signature algorithm and a certification request message (MRCA) including the control value (Sci), the operator identifier (Op_j) and the identifier (SN_i) is transmitted to a certification authority, which retrieves the identifier (Op_j) (1009) and the parent public key (KpM) value (1001). Verification (1012) of the message (MRCA) from the parent public key (KpM) and of the identifier of the on–board system (SN_i) enables to ensure that the public key (Kp) certification request and the use thereof originates indeed from an on–board component capable of restricting the use of said key.

(57) Abrégé

Un procédé et un système embarqué de vérification d'une requête de certification de clé publique (Kp) engendrée par un système embarqué d'identifiant (SN_i). Pour un ensemble (Lk) de systèmes embarqués, un opérateur habilité d'identifiant (OP_j) configure les systèmes embarqués et crée (1001) une clé publique mère (KpM) et une clé privée mère (KsM). L'identifiant (Op_j), la plage d'identifiants référencée (Lk) et la clé publique mère (KpM) sont publiés (1002). Pour chaque système embarqué (SN_i), une clé diversifiée (KsM_i) est créée à partir de l'identifiant (SN_i) et mémorisée (1003) en mémoire à accès protégé en lecture et écriture. Pour toute clé publique (Kp) engendrée par un système embarqué, une valeur de contrôle cryptographique (Sci) est calculée (1006) sur la clé publique (Kp), un identifiant d'algorithme (CAl) et des paramètres d'utilisation (U) de cette clé à l'aide d'un algorithme de signature à apport nul de connaissance et un message de requête de certification (MRCA) comprenant la valeur de contrôle (Sci), l'identifiant de l'opérateur (Op_j) et l'identifiant (SN_i) est transmis à une autorité de certification, laquelle retrouve l'identifiant (OP_j) (1009) et la valeur de la clé publique mère (KmP) (1011). Une vérification (1012) du message (MRCA) à partir de la clé publique mère (KpM) et de l'identifiant du système embarqué (SN_i) permet de s'assurer que la requête de certification de clé publique (Kp) et l'utilisation de celle–ci provient bien d'un composant embarqué à même de limiter l'utilisation de cette clé.

TRAITÉ DE COOPERATION EN MATIÈRE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE LA RECEPTION DE L'EXEMPLAIRE ORIGINAL

(règle 24.2.a) du PCT)

Destinataire:

CORLU, Bernard
Bull S.A.
PC58D20
68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

Date d'expédition (jour/mois/année)	**NOTIFICATION IMPORTANTE**
13 mars 2000 (13.03.00)	
Référence du dossier du déposant ou du mandataire	**Demande internationale no**
PCT 3775/BC	PCT/FR00/00332

Il est notifié au déposant que le Bureau international a reçu l'exemplaire original de la demande internationale précisée ci-après.

Nom(s) du ou des déposants et de l'Etat ou des Etats pour lesquels ils sont déposants:

BULL S.A. (pour tous les Etats désignés sauf US)
PINKAS, Denis (pour US seulement)

Date du dépôt international	:	10 février 2000 (10.02.00)
Date(s) de priorité revendiquée(s)	:	11 février 1999 (11.02.99)
Date de réception de l'exemplaire original par le Bureau international	:	28 février 2000 (28.02.00)
Liste des offices désignés	:	

EP :AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE
National :CA,JP,US

ATTENTION

Le déposant doit soigneusement vérifier les indications figurant dans la présente notification. En cas de divergence entre ces indications et celles que contient la demande internationale, il doit aviser immédiatement le Bureau international.

En outre, l'attention du déposant est appelée sur les renseignements donnés dans l'annexe en ce qui concerne

- [X] les délais dans lesquels doit être abordée la phase nationale
- [X] la confirmation des désignations faites par mesure de précaution
- [ ] les exigences relatives aux documents de priorité.

Une copie de la présente notification est envoyée à l'office récepteur et à l'administration chargée de la recherche internationale.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

n°de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé

Eugénia Santos

n°de téléphone (41-22) 338.83.38

RENSEIGNEMENTS CONCERNANT LES DELAIS DANS LESQUELS DOIT ETRE ABORDEE LA PHASE NATIONALE

Il est rappelé au déposant qu'il doit aborder la "phase nationale" auprès de chacun des offices désignés indiqués sur la notification de la réception de l'exemplaire original (formulaire PCT/IB/301) en payant les taxes nationales et en remettant les traductions, telles qu'elles sont prescrites par les législations nationales.

Le délai d'accomplissement de ces actes de procédure est de **20 MOIS** à compter dela date de priorité ou, pour les Etats désignés qui ont été élus par le déposant dans une demande d'examen préliminaire international ou dans une élection ultérieure, de **30 MOIS** à compter de la date de priorité, à condition que cette élection ait été effectuée avant l'expiration du 19e mois à compter de la date de priorité. Certains offices désignés (ou élus) ont fixé des délais qui expirent au-delà de 20 ou 30 mois à compter de la date de priorité. D'autres offices accordent une prolongation des délais ou un délai de grâce, dans certains cas moyennant le paiement d'une taxe supplémentaire.

En plus de ces actes de procédure, le déposant devra dans certains cas satisfaire à d'autres exigences particulières applicables dans certains offices. **Il appartient au déposant** de veiller à remplir en temps voulu les conditions requises pour l'ouverture de la phase nationale. La majorité des offices désignés n'envoient pas de rappel à l'approche de la date limite pour aborder la phase nationale.

Des informations détaillées concernant les actes de procédure à accomplir pour aborder la phase nationale auprès de chaque office désigné, les délais applicables et la possibilité d'obtenir une prolongation des délais ou un délai de grâce et toutes autres conditions applicables figurent dans le volume II du Guide du déposant du PCT. Les exigences concernant le dépôt d'une demande d'examen préliminaire international sont exposées dans le chapitre IX du volume I du Guide du déposant du PCT.

GR et ES sont devenues liées par le chapitre II du PCT le 7 septembre 1996 et le 6 septembre1997, respectivement, et peuvent donc être élues dans une demande d'examen préliminaire international ou dans une élection ultérieure présentée le 7 septembre 1996 (ou à une date postérieure) ou le 6 septembre 1997 (ou à une date postérieure), respectivement, quelle que soit la date de dépôt de la demande internationale (voir le second paragraphe, ci-dessus).

Veuillez noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

CONFIRMATION DES DESIGNATIONS FAITES PAR MESURE DE PRECAUTION

Seules les désignations expresses faites dans la requête conformément à la règle 4.9.a) figurent dans la présente notification. Il est important de vérifier si ces désignations ont été faites correctement. Des erreurs dans les désignations peuvent être corrigées lorsque des désignations ont été faites par mesure de précaution en vertu de la règle 4.9.b). Toute désignation ainsi faite peut être confirmée conformément aux dispositions de la règle 4.9.c) avant l'expiration d'un délai de 15 mois à compter de la date de priorité. En l'absence de confirmation, une désignation faite par mesure de précaution sera considérée comme retirée par le déposant. Il ne sera adressé aucun rappel ni invitation. Pour confirmer une désignation , il faut déposer une déclaration précisant l'Etat désigné concerné (avec l'indication de la forme de protection ou de traitement souhaitée) et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 15 mois.

EXIGENCES RELATIVES AUX DOCUMENTS DE PRIORITE

Pour les déposants qui n'ont pas encore satisfait aux exigences relatives aux documents de priorité, il est rappelé ce qui suit.

Lorsque la priorité d'une demande nationale, régionale ou internationale antérieure est revendiquée, le déposant doit présenter une copie de cette demande antérieure, certifiée conforme par l'administration auprès de laquelle elle a été déposée ("document de priorité"), à l'office récepteur (qui la transmettra au Bureau international) ou directement au Bureau international, avant l'expiration d'un délai de 16 mois à compter de la date de priorité, étant entendu que tout document de priorité peut être présenté au Bureau international avant la date de publication de la demande internationale, auquel cas ce document sera réputé avoir été reçu par le Bureau international le dernier jour du délai de 16 mois (règle 17.1.a)).

Lorsque le document de priorité est délivré par l'office récepteur, le déposant peut, au lieu de présenter ce document, demander à l'office récepteur de le préparer et de le transmettre au Bureau international. La requête à cet effet doit être formulée avant l'expiration du délai de 16 mois et peut être soumise au paiement d'une taxe (règle 17.1.b)).

Si le document de priorité en question n'est pas fourni au Bureau international, ou si la demande adressée à l'office récepteur de préparer et de transmettre le document de priorité n'a pas été faite (et la taxe correspondante acquittée, le cas échéant) avant l'expiration du délai applicable mentionné aux paragraphes précédents, tout Etat désigné peut ne pas tenir compte de la revendication de priorité; toutefois, aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Lorsque plusieurs priorités sont revendiquées, la date de priorité à prendre en considération aux fins du calcul du délai de 16 mois est la date du dépôt de la demande la plus ancienne dont la priorité est revendiquée.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur : le BUREAU INTERNATIONAL

PCT

NOTIFICATION RELATIVE A LA PRESENTATION OU A LA TRANSMISSION DU DOCUMENT DE PRIORITE

(instruction administrative 411 du PCT)

Destinataire:

CORLU, Bernard
Bull S.A.
PC58D20
68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

Date d'expédition (jour/mois/année) 13 mars 2000 (13.03.00)	
Référence du dossier du déposant ou du mandataire PCT 3775/BC	**NOTIFICATION IMPORTANTE**
Demande internationale no PCT/FR00/00332	Date du dépôt international (jour/mois/année) 10 février 2000 (10.02.00)
Date de publication internationale (jour/mois/année) Pas encore publiée	Date de priorité (jour/mois/année) 11 février 1999 (11.02.99)
Déposant BULL S.A. etc	

1. La date de réception (sauf lorsque les lettres "NR" figurent dans la colonne de droite) par le Bureau international du ou des documents de priorité correspondant à la ou aux demandes énumérées ci-après est notifiée au déposant. Sauf indication contraire consistant en un astérisque figurant à côté d'une date de réception, ou les lettres "NR", dans la colonne de droite, le document de priorité en question a été présenté ou transmis au Bureau international d'une manière conforme à la règle 17.1.a) ou b).
2. Ce formulaire met à jour et remplace toute notification relative à la présentation ou à la transmission du document de priorité qui a été envoyée précédemment.
3. Un **astérisque(*)** figurant à côté d'une date de réception dans la colonne de droite signale un document de priorité présenté ou transmis au Bureau international mais de manière non conforme à la règle 17.1.a) ou b). Dans ce cas, **l'attention du déposant est appelée** sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.
4. Les **lettres "NR"** figurant dans la colonne de droite signalent un document de priorité que le Bureau international n'a pas reçu ou que le déposant n'a pas demandé à l'office récepteur de préparer et de transmettre au Bureau international, conformément à la règle 17.1.a) ou b), respectivement. Dans ce cas, **l'attention du déposant est appelée** sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Date de priorité	Demande de priorité n°	Pays, office régional ou office récepteur selon le PCT	Date de réception du document de priorité
11 févr 1999 (11.02.99)	99/01652	FR	28 févr 2000 (28.02.00)

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:

Eugénia Santos

no de téléphone (41-22) 338.83.38

PCT

REQUÊTE

Le soussigné requiert que la présente demande internationale soit traitée conformément au Traité de coopération en matière de brevets.

Réservé à l'office récepteur

Demande internationale n°

Date du dépôt international

Nom de l'office récepteur et "Demande internationale PCT"

Référence du dossier du déposant ou du mandataire *(facultatif)* *(12 caractères au maximum)* PCT 3775/BC

Cadre n° I TITRE DE L'INVENTION

Procédé de vérification de l'usage de clés publiques engendrées par un système embarqué.

Cadre n° II DÉPOSANT

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

BULL S.A.

68, route de Versailles
78434 LOUVECIENNES CEDEX
FRANCE

☐ Cette personne est aussi inventeur.

n° de téléphone (33) 1 39.66.61.76

n° de télécopieur (33) 1 39.66.61.73

n° de téléimprimeur

Nationalité (nom de l'État) : FRANCE

Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☒ tous les États désignés sauf les États-Unis d'Amérique ☐ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

Cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

PINKAS Denis

13 Pavé des Gardes
92370 CHAVILLE
FRANCE

Cette personne est :

☐ déposant seulement

☒ déposant et inventeur

☐ inventeur seulement
(Si cette case est cochée, ne pas remplir la suite.)

Nationalité (nom de l'État) : FRANCE

Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☒ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

☐ D'autres déposants ou inventeurs sont indiqués sur une feuille annexe.

Cadre n° IV MANDATAIRE OU REPRÉSENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE

La personne dont l'identité est donnée ci-dessous est/a été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme: ☒ mandataire ☐ représentant commun

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)*

BULL S.A
CORLU Bernard
PC58D20 / 68, route de Versailles
78434 LOUVECIENNES CEDEX

n° de téléphone (33) 1 39.66.61.76

n° de télécopieur (33) 1 39.66.61.73

n° de téléimprimeur

☐ **Adresse pour la correspondance :** cocher cette case lorsque aucun mandataire ni représentant commun n'est/n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.

PCT 754/301293

Cadre n° V DÉSIGNATION D'É[redacted]

Les désignations suivantes sont faites c[redacted]rmément à la règle 4.9.a) *(cocher les cases appropriées: une au moins doit l'être)* :

Brevet régional

☐ **AP** **Brevet ARIPO** : **GH** Ghana, **GM** Gambie, **KE** Kenya, **LS** Lesotho, **MW** Malawi, **SD** Soudan, **SL** Sierra Leone, **SZ** Swaziland, **TZ** République-Unie de Tanzanie, **UG** Ouganda, **ZW** Zimbabwe et tout autre État qui est un État contractant du Protocole de Harare et du PCT

☐ **EA** **Brevet eurasien** : **AM** Arménie, **AZ** Azerbaïdjan, **BY** Bélarus, **KG** Kirghizistan, **KZ** Kazakhstan, **MD** République de Moldova, **RU** Fédération de Russie, **TJ** Tadjikistan, **TM** Turkménistan et tout autre État qui est un État contractant de la Convention sur le brevet eurasien et du PCT

☒ **EP** **Brevet européen** : **AT** Autriche, **BE** Belgique, **CH et LI** Suisse et Liechtenstein, **CY** Chypre, **DE** Allemagne, **DK** Danemark, **ES** Espagne, **FI** Finlande, **FR** France, **GB** Royaume-Uni, **GR** Grèce, **IE** Irlande, **IT** Italie, **LU** Luxembourg, **MC** Monaco, **NL** Pays-Bas, **PT** Portugal, **SE** Suède et tout autre État qui est un État contractant de la Convention sur le brevet européen et du PCT

☐ **OA** **Brevet OAPI** : **BF** Burkina Faso, **BJ** Bénin, **CF** République centrafricaine, **CG** Congo, **CI** Côte d'Ivoire, **CM** Cameroun, **GA** Gabon, **GN** Guinée, **GW** Guinée-Bissau, **ML** Mali, **MR** Mauritanie, **NE** Niger, **SN** Sénégal, **TD** Tchad, **TG** Togo et tout autre État qui est un État membre de l'OAPI et un État contractant du PCT *(si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)* . . . . . .

Brevet national *(si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)* :

☐ **AE** Émirats arabes unis
☐ **AL** Albanie . . . . . .
☐ **AM** Arménie . . . . . .
☐ **AT** Autriche . . . . . .
☐ **AU** Australie . . . . . .
☐ **AZ** Azerbaïdjan
☐ **BA** Bosnie-Herzégovine . . . . . .
☐ **BB** Barbade
☐ **BG** Bulgarie . . . . . .
☐ **BR** Brésil . . . . . .
☐ **BY** Bélarus . . . . . .
☒ **CA** Canada
☐ **CH et LI** Suisse et Liechtenstein
☐ **CN** Chine . . . . . .
☐ **CR** Costa Rica . . . . . .
☐ **CU** Cuba . . . . . .
☐ **CZ** République tchèque . . . . . .
☐ **DE** Allemagne . . . . . .
☐ **DK** Danemark . . . . . .
☐ **DM** Dominique
☐ **EE** Estonie . . . . . .
☐ **ES** Espagne . . . . . .
☐ **FI** Finlande . . . . . .
☐ **GB** Royaume-Uni
☐ **GD** Grenade
☐ **GE** Géorgie . . . . . .
☐ **GH** Ghana . . . . . .
☐ **GM** Gambie
☐ **HR** Croatie . . . . . .
☐ **HU** Hongrie . . . . . .
☐ **ID** Indonésie
☐ **IL** Israël . . . . . .
☐ **IN** Inde . . . . . .
☐ **IS** Islande
☒ **JP** Japon . . . . . .
☐ **KE** Kenya . . . . . .
☐ **KG** Kirghizistan . . . . . .
☐ **KP** République populaire démocratique de Corée . . . . . .
☐ **KR** République de Corée . . . . . .
☐ **KZ** Kazakhstan . . . . . .
☐ **LC** Sainte-Lucie
☐ **LK** Sri Lanka
☐ **LR** Liberia
☐ **LS** Lesotho . . . . . .
☐ **LT** Lituanie
☐ **LU** Luxembourg
☐ **LV** Lettonie
☐ **MA** Maroc . . . . . .
☐ **MD** République de Moldova . . . . . .
☐ **MG** Madagascar . . . . . .
☐ **MK** Ex-République yougoslave de Macédoine . . . . . .
☐ **MN** Mongolie
☐ **MW** Malawi . . . . . .
☐ **MX** Mexique . . . . . .
☐ **NO** Norvège
☐ **NZ** Nouvelle-Zélande . . . . . .
☐ **PL** Pologne . . . . . .
☐ **PT** Portugal . . . . . .
☐ **RO** Roumanie
☐ **RU** Fédération de Russie . . . . . .
☐ **SD** Soudan
☐ **SE** Suède
☐ **SG** Singapour
☐ **SI** Slovénie . . . . . .
☐ **SK** Slovaquie . . . . . .
☐ **SL** Sierra Leone . . . . . .
☐ **TJ** Tadjikistan . . . . . .
☐ **TM** Turkménistan . . . . . .
☐ **TR** Turquie . . . . . .
☐ **TT** Trinité-et-Tobago . . . . . .
☐ **TZ** République-Unie de Tanzanie
☐ **UA** Ukraine . . . . . .
☐ **UG** Ouganda . . . . . .
☒ **US** États-Unis d'Amérique . . . . . .
☐ **UZ** Ouzbékistan . . . . . .
☐ **VN** Viet Nam . . . . . .
☐ **YU** Yougoslavie . . . . . .
☐ **ZA** Afrique du Sud . . . . . .
☐ **ZW** Zimbabwe . . . . . .

Cases réservées pour la désignation d'États qui sont devenus parties au PCT après la publication de la présente feuille :

☐ . . . . . .
☐ . . . . . .

Déclaration concernant les désignations de précaution : outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, à l'exception de toute désignation indiquée dans le cadre supplémentaire comme étant exclue de la portée de cette déclaration. Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. *(La confirmation (y compris les taxes) doit parvenir à l'office récepteur dans le délai de 15 mois.)*

Cadre n° VI REVENDICATION DE PRIORITÉ ☐ D'autres revendications de priorité sont indiquées dans le cadre supplémentaire.

Date de dépôt de la demande antérieure *(jour/mois/année)*	Numéro de la demande antérieure	Lorsque la demande antérieure est une : demande nationale : pays	demande régionale : * office régional	demande internationale : office récepteur
(1) 11 février 1999 (11.02.1999)	99 01652	FRANCE		
(2)				
(3)				

☒ L'office récepteur est prié de préparer et de transmettre au Bureau international une copie certifiée conforme de la ou des demandes antérieures *(seulement si la demande antérieure a été déposée auprès de l'office qui, aux fins de la présente demande internationale, est l'office récepteur)* indiquées ci-dessus au(x) point(s) : 1

* *Si la demande antérieure est une demande ARIPO, il est obligatoire d'indiquer dans le cadre supplémentaire au moins un pays partie à la Convention de Paris pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée (règle 4.10.b)ii)). Voir le cadre supplémentaire.*

Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Choix de l'administration chargée de la recherche internationale (ISA) *(si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres peut être utilisé)* :
ISA/

Demande d'utilisation des résultats d'une recherche antérieure; mention de cette recherche *(si une recherche antérieure a été effectuée par l'administration chargée de la recherche internationale ou demandée à cette dernière)* :

Date *(jour/mois/année)*	Numéro	Pays *(ou office régional)*
11.02.99	99 01652 FA 578458	FR

Cadre n° VIII BORDEREAU; LANGUE DE DÉPÔT

La présente demande internationale contient le **nombre de feuilles** suivant :

requête	:	03
description (sauf partie réservée au listage des séquences)	:	30
revendications	:	05
abrégé	:	01
dessins	:	06
partie de la description réservée au listage des séquences	:	
Nombre total de feuilles	:	45

Le ou les éléments cochés ci-après **sont joints** à la présente demande internationale :

1. ☐ feuille de calcul des taxes
2. ☒ pouvoir distinct signé
3. ☐ copie du pouvoir général; numéro de référence, le cas échéant :
4. ☐ explication de l'absence d'une signature
5. ☒ document(s) de priorité indiqué(s) dans le cadre n° VI au(x) point(s) : 1
6. ☐ traduction de la demande internationale en (langue) :
7. ☐ indications séparées concernant des micro-organismes ou autre matériel biologique déposés
8. ☐ listage des séquences de nucléotides ou d'acides aminés sous forme déchiffrable par ordinateur
9. ☐ autres éléments *(préciser)* : Rapport de Recherche FA578458 non publié

Figure des dessins qui doit accompagner l'abrégé : 2A

Langue de dépôt de la demande internationale : FRANCAIS

Cadre n° IX SIGNATURE DU DÉPOSANT OU DU MANDATAIRE

À côté de chaque signature, indiquer le nom du signataire et, si cela n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe.

CORLU Bernard (mandataire)

Réservé à l'office récepteur

1. Date effective de réception des pièces supposées constituer la demande internationale :
2. Dessins : ☐ reçus : ☐ non reçus :
3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :
4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2) du PCT :
5. Administration chargée de la recherche internationale (si plusieurs sont compétentes) : ISA/
6. ☐ Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche.

Réservé au Bureau international

Date de réception de l'exemplaire original par le Bureau international :

PROCEDE DE VERIFICATION DE L'USAGE DE CLES PUBLIQUES ENGENDREES PAR UN SYSTEME EMBARQUE

L'invention concerne un procédé de vérification, notamment de l'usage de clés publiques engendrées par un système embarqué, et le système embarqué correspondant.

Afin d'assurer la sécurité de transmission des données transmises sur les réseaux informatiques, les utilisateurs de ces réseaux ont exercé une forte demande relative à des prestations de chiffrement/déchiffrement et/ou de génération/vérification de signature numérique de ces données transmises.

Les opérations de chiffrement/déchiffrement ont pour but de coder puis de décoder, à partir d'une convention secrète temporairement partagée entre un émetteur et un récepteur, des messages transmis afin de rendre ces derniers inintelligibles aux tiers à cette convention.

Les opérations de signature ont pour objet la transmission de messages spécifiques permettant de s'assurer de l'intégrité et l'origine des données transmises.

Pour des raisons de sécurité publique, les Pouvoirs Publics ont, dans certains états, mis en place des dispositions législatives contraignantes afin d'imposer une réglementation stricte des opérations de chiffrement/déchiffrement utilisant des algorithmes dits "forts". Toutefois, les autres opérations telles le chiffrement/déchiffrement utilisant des algorithmes dits "faibles", l'authentification, l'intégrité et la non-répudiation utilisant un calcul de signature numérique ne font pas l'objet de telles mesures contraignantes. En particulier, le message d'information accompagnant une

signature numérique étant transmis en clair peut faire l'objet de tout contrôle de police utile.

Différents systèmes de calcul de signatures numériques ont, jusqu'à ce jour, été proposés.

Parmi ceux-ci, les systèmes cryptographiques à clés asymétriques ont été plus particulièrement développés en raison de leur souplesse d'utilisation ou tout au moins de la souplesse relative de gestion des clés précitées. En effet, ces systèmes mettent en œuvre une clé privée, non publiée, et une clé publique. La connaissance de la clé publique ne permet pas de calculer la clé privée.

Certains algorithmes de signature numérique ne peuvent servir à un autre usage que la signature numérique. C'est ainsi le cas du système connu sous le nom de DSA (Digital Signature Algorithm). Cependant il existe un autre algorithme largement utilisé connu sous le nom de RSA, du nom de leurs inventeurs RIVEST, SHAMIR et ADLEMAN, lequel permet à la fois la mise en œuvre d'opérations de calcul de signature numérique et de chiffrement/déchiffrement, dit "fort".

La présente invention a, en autres objets, dans le cadre de la mise en œuvre d'un système cryptographique à clés asymétriques, de s'assurer qu'un système embarqué utilisant l'algorithme RSA et des clés RSA à usage de signature seulement sera en mesure de supporter uniquement des opérations de signature à partir de cesdites clés et en aucun cas des opérations de déchiffrement.

Un autre objet de la présente invention est la mise en place d'une infrastructure de clés publiques utilisable exclusivement à des fins de signature numérique. En effet, si un utilisateur tentait d'utiliser à des fins de chiffrement l'une des clés publiques RSA ainsi certifiées à des fins de signature, l'entité en possession de la clé

privée RSA correspondante se trouverait dans la totale incapacité de pouvoir déchiffrer en utilisant ladite clé privée.

Un autre objet de la présente invention est également un procédé de vérification d'une requête de certification de clé publique engendrée par un système embarqué permettant un contrôle, par une autorité de certification, de l'usage de cette clé à des fins d'opérations de déchiffrement limitées.

Un autre objet de la présente invention est enfin, dans le cadre du contrôle précité de l'usage de cette clé, la limitation de cet usage à des opérations de chiffrement/déchiffrement au moyen d'algorithmes symétriques "faibles" autorisés par certains pouvoirs publics.

On rappelle que les systèmes embarqués sont, de manière générale, constitués par une carte à microprocesseur et mis à la disposition d'une entité.

La notion d'entité précitée recouvre soit la personne physique titulaire d'un système embarqué telle qu'une carte à microprocesseur, soit tout système informatique muni d'un système embarqué ou carte à microprocesseur comparable.

Le procédé de vérification de l'origine de la requête de certification d'une clé publique issue d'un jeu de clés asymétriques, clé publique Kp et clé privée Ks engendrées, pour un algorithme donné CAl et pour un usage donné, tel que le chiffrement/déchiffrement ou la vérification/ génération de signature numérique, par un système embarqué et mémorisées dans la zone mémoire d'un système embarqué Si muni de moyens de calcul cryptographique et de moyens de mémorisation de données numériques à accès externe protégé en écriture/lecture, ces

données numériques IDd_i comportant au moins un numéro de série SN_i permettant l'identification du système embarqué et un code d'identification OP_j d'un opérateur habilité à configurer ledit système embarqué et cette requête étant formulée par ledit système embarqué par transmission d'un message de requête MRCA contenant ladite clé publique Kp à une autorité de certification CA est remarquable en ce qu'il consiste, préalablement à toute transmission d'une requête de certification, lors de la configuration de ces systèmes embarqués par cet opérateur habilité, pour tous les systèmes embarqués Si d'un ensemble Lk de systèmes embarqués :

- à faire engendrer par cet opérateur habilité, pour cet ensemble donné de systèmes embarqués, une clé publique mère KpM et une clé privée mère KsM ;
- à publier ladite clé publique mère KpM associée d'une part à l'identité de cet opérateur habilité OP_j et d'autre part à cet ensemble Lk de systèmes embarqués ; et

pour chaque système embarqué appartenant à la plage d'identifiants définie par l'ensemble Lk de systèmes embarqués :

- à faire engendrer par cet opérateur habilité, à partir de ladite clé privée mère KsM et du numéro de série SN_i du système embarqué, une clé privée diversifiée KsM_i et à mémoriser, dans ladite zone mémoire à accès externe protégé en écriture/lecture, ladite clé privée diversifiée KsM_i, et préalablement à toute transmission d'une requête de certification,
- à faire engendrer par l'intermédiaire du système embarqué une requête de certification RCA, contenant en particulier un champ de clé publique CAl,Kp et les indicateurs d'usage U de cette clé publique;

- à faire engendrer par l'intermédiaire du système embarqué, au moyen desdits moyens de calcul et de ladite clé diversifiée KsM_i, associée à ce système embarqué, une valeur de contrôle cryptographique Sc_i sur l'ensemble de la requête RCA, cette valeur de contrôle cryptographique étant une signature numérique calculée au moyen de la clé privée diversifiée KsM_i ; et lors de l'émission, par le système embarqué, d'une requête de certification à l'autorité de certification :

- à former un message de requête de certification MRCA contenant la requête RCA, l'identifiant IDd_i du système embarqué, ce dernier étant constitué d'une part de l'identifiant OP_j de cet opérateur habilité et d'autre part du numéro de série SN_i du système embarqué, et la valeur de contrôle cryptographique Sci,

- à transmettre à l'autorité de certification CA ledit message de requête MRCA formé lors de l'étape précédente et contenant les champs de clé publique CAl,Kp et les indicateurs d'usage U, objets de ladite certification, et ladite valeur de contrôle cryptographique Sc_i ;

- à retrouver, lors de la réception d'un message de requête de certification MRCA par l'autorité de certification, l'identité de l'opérateur habilité OP_J à partir de l'identifiant IDd_i du système embarqué,

- à retrouver, à partir de l'identifiant OP_j de l'opérateur habilité, la valeur de la clé publique mère KpM associée à l'ensemble Lk auquel appartient le système embarqué ;

- à vérifier, à partir de ladite clé publique mère KpM, dudit numéro de série SN_i du système embarqué, dudit message de requête de certification reçue MRCA, ladite valeur de contrôle cryptographique Sc_i, ce qui permet

d'établir l'authenticité de cette valeur de contrôle cryptographique et de l'origine de cette requête de certification.

Le procédé de vérification d'une requête de certification de clé engendrée par un système embarqué, objet de l'invention, s'applique à tout type de système embarqué, mais plus particulièrement à des systèmes embarqués en nombre constitués chacun par une carte à microprocesseur ou analogue.

Il sera mieux compris à la lecture de la description et à l'observation des dessins ci-après dans lesquels, outre la figure 1 relative à un système embarqué, constitué par une carte à microprocesseur de type classique,

- la figure 2a représente, à titre d'exemple non limitatif, un organigramme de l'ensemble des opérations ou étapes permettant la mise en œuvre du procédé objet de la présente invention, c'est à dire de la génération d'une requête de certification générée par le système embarqué;

- la figure 2b représente, à titre d'exemple non limitatif, un organigramme d'une variante de mise en œuvre du procédé, objet de la présente invention, tel que représenté en figure 2a et dans lequel un contrôle de la syntaxe d'un gabarit de requête de certification fournie au système embarqué est effectué par le système embarqué, préalablement à la génération de ladite requête de certification ;

- la figure 3 représente, sous forme d'un diagramme fonctionnel, le détail de l'étape du procédé mis en œuvre ainsi qu'illustré en figure 2a ou 2b, dans laquelle une clé privée diversifiée est calculée pour chaque système embarqué ;

- la figure 4a représente, à titre d'exemple non limitatif, la structure d'un message de requête de certification dans une version simplifiée, permettant la mise en œuvre du procédé objet de l'invention tel que représenté en figure 2a ;

- la figure 4b représente, à titre d'exemple non limitatif, la structure d'un message de requête de certification dans une version améliorée et codé au format ASN1 selon une structure TLV, plus particulièrement destinée à la mise en œuvre du procédé objet de l'invention tel que représenté en figure 2b ;

- la figure 5 représente, sous forme d'un diagramme fonctionnel, le détail de l'étape du procédé mis en œuvre ainsi qu'illustré en figure 2a ou 2b, dans laquelle une vérification du message de requête est effectuée par l'autorité de certification ;

- la figure 6 représente une variante particulièrement avantageuse de mise en œuvre du procédé objet de la présente invention, dans laquelle à la clé privée associée à une clé publique, objet d'une requête de certification, est associée une clé symétrique de chiffrement/déchiffrement faible, au système embarqué correspondant étant ainsi conféré une fonction de chiffrement/déchiffrement faible, satisfaisant aux dispositions légales en vigueur dans certains pays en vue d'une commercialisation de ces systèmes en l'absence d'une autorisation préalable ;

- la figure 7 représente un système embarqué permettant la mise en œuvre du procédé objet de l'invention.

Une description plus détaillée du procédé de vérification de la requête de certification d'une clé publique conforme à l'objet de la présente invention sera

maintenant donnée en liaison avec les figures 2a, 2b et les figures suivantes.

Préalablement à la description détaillée des étapes nécessaires à la mise en œuvre du procédé en liaison avec les figures précitées, des considérations d'ordre général visant à illustrer le contexte de mise en œuvre du procédé, objet de la présente invention, seront données ci-après.

D'une manière générale, le procédé objet de la présente invention permet d'assurer la vérification d'une requête de certification de clé publique engendrée par un système embarqué, cette vérification comportant notamment la vérification de l'origine de cette requête, mais également compte tenu de la vérification ainsi effectuée et de la certitude ainsi obtenue de l'origine de cette requête, d'avoir la certitude que la clé privée correspondant à la clé publique générée faisant l'objet de la présente requête de certification ne pourra servir qu'à des usages bien spécifiés, telle la génération de signature numérique ou le déchiffrement de clés symétriques faibles.

Les clés publiques étant, comme leur nom l'indique, publiques, il ne saurait être question de pouvoir limiter l'usage de ces clés pour le chiffrement. Cependant les clés privées étant nécessairement protégées, le mécanisme de protection mis en œuvre pourra être en mesure d'empêcher l'usage de clés privées RSA à des fins de déchiffrement. Si donc l'opération de chiffrement ne peut être interdite, l'opération de déchiffrement peut l'être et donc le processus de chiffrement/déchiffrement devient ainsi impossible. La procédure mise en œuvre s'appuie sur le fait qu'il est possible de s'assurer que la clé privée correspondant à une clé publique donnée ne pourra être utilisée à des fins de déchiffrement de par le fait qu'il est possible d'être sûr qu'elle est effectivement contenue

dans un système embarqué protégé empêchant son usage à des fins de déchiffrement.

Afin de s'assurer qu'une clé donnée est attachée à une entité donnée, une technique de certification des clés est actuellement largement utilisée. Cette technique consiste à faire engendrer par une Autorité de Certification AC un certificat de clé publique qui associe à un nom d'entité donné, un identifiant d'algorithme à clé publique CAl, une valeur de clé publique Kp, pour des usages donnés U et ce, pour une période de validité donnée. Un exemple de tel certificat est connu sous le nom de certificat X.509 du nom de la norme de l'ITU (International Telecommunications Union) qui l'a normalisé.

Afin de pouvoir participer à une architecture supportant des clés publiques il est nécessaire de pouvoir disposer d'un certificat de clé publique. Pour cela il est nécessaire de formuler une requête qui comporte les informations que le demandeur souhaite voir figurer dans son certificat. Cette requête comporte en particulier l'identifiant de l'algorithme utilisé CAl, la valeur de la clé publique Kp pour cet algorithme et les usages de cette clé U. Si la requête émane directement de l'entité il est impossible de connaître les protections mises en œuvre pour la clé privée correspondante. Cependant si la requête émane directement d'un système embarqué protégé empêchant l'usage de la clé privée à des fins de déchiffrement, alors il est possible de s'assurer que la clé privée correspondant à la clé publique qui fait l'objet de la demande de certification ne pourra être utilisable que pour les usages indiqués, par exemple à des fins de génération de signature ou de déchiffrement de clés faibles. C'est l'un des objets du procédé objet de la présente invention, lequel sera

décrit ci-après en détail en liaison avec les figures 2a et 2b.

Le procédé, objet de la présente invention, sera décrit maintenant dans le cas non limitatif où le système embarqué est constitué par une carte à microprocesseur telle qu'une carte bancaire, une carte PCMCIA analogue.

De manière classique, ainsi que représenté sur la figure 1, une carte à microprocesseur 10 comprend un système d'entrée/sortie 12, reliée au microprocesseur 14, une mémoire RAM 16, une mémoire non volatile 18, constituée par une mémoire morte ROM 18b et une mémoire programmable 18a. L'ensemble de ces éléments est relié au microprocesseur 14 par une liaison par BUS. Un module 20 de calcul cryptographique de données est, en outre, ajouté. La mémoire non volatile 18 comporte habituellement une zone mémoire à accès protégé en écriture/lecture, notée MAP, l'accès de cette zone étant réservé au seul microprocesseur 14 à des fins d'utilisation purement interne.

En référence à la figure 1, on indique que dans une telle carte à microprocesseur, le module de calcul cryptographique peut contenir des programmes de génération ou vérification de signature, de chiffrement/déchiffrement mis en œuvre à partir de processus dits "forts" supportés par l'algorithme RSA par exemple, ainsi que des processus dits "faibles" supportés par des algorithmes tel que le DES limité à des tailles de clé de 40 bits par exemple.

Conformément à la figure 2a, un opérateur habilité, identifié par un identifiant OP_j est en situation à l'étape 1000 de procéder à une configuration d'un ensemble de systèmes embarqués, cet ensemble étant noté Lk. D'une manière pratique, on indique que cet ensemble correspond à un lot de systèmes embarqués tel que des cartes à microprocesseur par exemple, que cet opérateur souhaite

distribuer dans le commerce. Cet opérateur habilité peut bien entendu être soit le fabricant de cartes à mémoire soit tout sous-traitant habilité par ce dernier ou par une autorité publique ou privée agréée. Chaque système embarqué est en outre doté d'un numéro d'identification noté SN_i et, dans le cadre de la mise en œuvre du procédé, objet de la présente invention, chaque système embarqué S_i appartenant à l'ensemble Lk donné est donc muni d'un numéro d'identification, noté IDd_i constitué par l'identifiant de l'opérateur habilité OP_j et par le numéro de série SN_i de ce système embarqué.

Afin de vérifier notamment l'origine de la requête de certification d'une clé publique issue d'un jeu de clés asymétriques, clé publique Kp et clé privée Ks, engendrées par un système embarqué appartenant à l'ensemble de systèmes embarqués précité, ces clés publique Kp et privée Ks étant engendrées pour un usage donné tel que le chiffrement/déchiffrement ou la vérification/génération de signature numérique par exemple, le procédé objet de la présente invention consiste, préalablement à toute transmission d'une requête de certification, lors d'une étape de configuration des systèmes embarqués par l'opérateur habilité à réaliser cette configuration, à faire engendrer, en une étape 1001, par cet opérateur habilité et pour l'ensemble de systèmes embarqués, une clé publique mère, notée KpM, et une clé privée mère KsM destinées à être mises en œuvre dans le cadre d'un processus supporté par l'algorithme CalM relatif aux clés KpM et KsM.

L'étape 1001 précitée, suivie d'une étape 1002 consistant à publier la clé publique mère KpM associée d'une part à l'identité de l'opérateur habilité OP_j et d'autre part à l'ensemble Lk de systèmes embarqués. Ainsi

que représenté à l'étape 1002 sur la figure 2a, cette publication peut consister en une publication de quatre valeurs liées sous forme d'une liste par exemple, c'est-à-dire de l'identifiant de l'opérateur habilité OP_j, d'une plage d'identifiants définie par l'ensemble Lk et bien entendu de la valeur de la clé publique mère KpM associée au code indicateur de l'algorithme à mettre en œuvre CAlM. La plage d'identifiants peut être constituée par un identifiant de début et de fin de plage.

Lors de cette étape de configuration par l'opérateur habilité, on indique que la création des clés, clé publique mère KpM et clé privée mère KsM, est directement dépendante de l'algorithme utilisé et ne peut donc être décrite de manière indépendante du processus supporté par l'algorithme mis en œuvre. Le type d'algorithme à mettre en œuvre est cependant précisé ci-après.

A la suite de l'étape 1002 précitée, le procédé, objet de la présente invention consiste, pour chaque système embarqué Si appartenant à l'ensemble Lk des systèmes embarqués, à calculer en une étape 1003, à partir de la clé privée mère KsM et du numéro de série SN_i de chaque système embarqué considéré S_i, une clé privée diversifiée, notée KsM_i.

Conformément à un aspect particulièrement avantageux du procédé, objet de la présente invention, la clé privée diversifiée KsM_i est alors mémorisée dans la zone mémoire à accès externe protégé en lecture/écriture MAP de la carte à microprocesseur constituant le système embarqué.

D'une manière générale, on indique que la clé privée diversifiée KsM_i est unique et distincte pour chaque

système embarqué dont l'identifiant SN_i est différent dans l'ensemble Lk.

Suite à l'étape 1003 précédemment mentionnée, le procédé, objet de la présente invention, consiste, dans une version avantageuse, préalablement à toute transmission d'une requête de certification et pour toute clé publique Kp à certifier à la demande de chaque système embarqué Si considéré, cette demande étant bien entendu formulée par un utilisateur Uti, c'est-à-dire par une entité, à faire engendrer, en une étape 1004-5, par l'intermédiaire du système embarqué, une requête de certification RCA contenant en particulier un champ de clé publique CAl,Kp et les indicateurs d'usage U de cette clé publique. Lorsque la requête de certification RCA est engendrée directement par le système embarqué, le procédé peut consister à engendrer, au niveau du système embarqué, la requête de certification RCA. Celle-ci est alors composée de trois champs, soit un identifiant d'algorithme à clé publique CAl, une valeur de clé publique Kp et un indicateur des usages de cette clé U.

Dans un mode de réalisation spécifique non limitatif, l'étape 1004-5 peut par exemple consister à communiquer, en une étape 1004, au système embarqué d'identifiant SN_i considéré, un gabarit de requête de certification, noté GRCA, ce gabarit contenant tous les champs requis hormis les champs de clé publique de déchiffrement ou de vérification de signature numérique ainsi que les indicateurs d'usage U de la clé publique Kp, objets de la certification demandée.

La vérification du gabarit de requête de certification GRCA sera décrite de manière plus détaillée ultérieurement dans la description.

Le gabarit de requête de certification GRCA permet alors, en une étape 1005, au système embarqué considéré,

d'effectuer une opération consistant à compléter les champs manquants du gabarit de requête de certification GRCA. Ainsi, le champ de clé publique, champ comportant l'identifiant d'un algorithme CAl de chiffrement/déchiffrement ou de calcul de signature, par exemple l'algorithme RSA précité, et une valeur de clé publique Kp, objet de la certification demandée, ainsi que le champ relatif aux indicateurs d'usage U de cette clé publique sont complétés afin de reconstituer une requête de certification complète, notée RCA, à l'étape 1005 suivante.

Sur la figure 2a, on a représenté l'étape 1005 comme consistant à faire effectuer le complément par le système embarqué des champs manquants précités, le symbole + représentant cette opération de complément. D'une manière générale, on indique que l'opération de complément précitée peut consister soit à attribuer des valeurs adéquates à des valeurs fictives déjà présentes dans le gabarit de requête de certification GRCA dans des champs déterminés, soit le cas échéant à compléter ce gabarit de requête par des opérations de concaténation au moyen de ces valeurs adéquates ainsi qu'il sera décrit ultérieurement dans la description.

L'étape 1004-5 ou l'étape 1005 précitée est alors suivie d'une étape 1006 consistant à calculer, grâce à la mise en œuvre du module de calcul du système embarqué considéré et de la clé diversifiée KsM_i associée à ce système embarqué à l'étape 1003, une valeur de contrôle cryptographique, notée Sc_i.

D'une manière générale, on indique que la valeur de contrôle cryptographique précitée est calculée sur l'ensemble de la requête complétée RCA ainsi que sur l'identifiant IDd_i du système embarqué considéré. On rappelle que l'identifiant IDd_i du système embarqué Si est

constitué par l'identifiant Op_j de l'opérateur habilité et par le numéro de série SN_i du système embarqué.

De préférence, la valeur de contrôle cryptographique Sc_i est une signature numérique calculée au moyen de la clé privée diversifiée KsM_i.

Pour cette raison la valeur de contrôle cryptographique vérifie la relation :

$$Sc_i = S_{KsMi}\ (RCA, IDd_i)$$

Dans cette relation, on indique que l'indice KsMi affecté à l'opération de signature S indique le calcul de cette signature à partir de la clé privée diversifiée KsM_i sur les arguments RCA et IDd_i.

Le procédé, objet de la présente invention, consiste alors, lors de l'émission par le système embarqué considéré d'une requête de certification à l'autorité de certification, cette opération étant notée "Requête par Ut_i" sur la figure 2a, à former, à l'extérieur du système embarqué, en une étape 1007, un message de requête de certification, noté MRCA, composé de la requête complétée RCA par le système embarqué considéré, de l'identifiant du système embarqué, ainsi que de la valeur de contrôle cryptographique Sc_i considérée.

Suite à l'étape 1007 précitée, une étape 1008 est prévue, laquelle consiste à transmettre à l'autorité de certification CA le message de requête MRCA formé lors de l'étape 1007 précédente. Le message MRCA contient en particulier la requête de certification complétée de la clé publique Kp dont la certification est demandée ainsi que de ses indicateurs d'usage U, cette clé publique Kp et ces indicateurs d'usage étant ainsi l'objet de la certification demandée précitée.

Le procédé, objet de la présente invention, consiste ensuite, lors de la réception d'un message de

requête de certification MRCA précité, pour l'autorité de certification, à effectuer les opérations consistant à l'étape 1009 à retrouver l'identité de l'opérateur habilité OP_j ainsi que l'identifiant SN_i du système embarqué à partir de l'identifiant IDd_i du système embarqué, puis, à l'étape 1010, à retrouver, la plage d'identifiants Lk à laquelle appartient l'identifiant SN_i à partir des données publiées par l'opérateur Opj, puis, à l'étape 1011 à retrouver à partir des données de l'ensemble Lk, l'identifiant du processus supporté par l'algorithme à mettre en œuvre CAlM, la valeur de la clé publique mère KpM associée à l'ensemble Lk.

On comprend en particulier qu'aux étapes 1009, 1010 et 1011, la publication à l'étape 1002 des variables liées OP_j identifiant de l'opérateur habilité, Lk identifiant de l'ensemble considéré, CAlM identifiant l'algorithme à mettre en œuvre, et KpM valeur de la clé publique mère associée à cet ensemble de systèmes embarqués, permette de retrouver successivement l'identifiant de cet opérateur habilité puis la valeur de la clé publique KpM ainsi que l'identifiant de l'algorithme à mettre en œuvre CAlM par exemple à partir des quatre variables liées publiées.

Suite à l'obtention par l'autorité de certification de la valeur de la clé publique mère KpM précitée, une étape 1012 est alors réalisée, laquelle consiste à vérifier, à partir de la valeur de la clé publique mère KpM, du numéro de série SN_i du système embarqué et de la requête de certification complète reçue RCA, la valeur de contrôle cryptographique Sc_i. L'opération de vérification de la valeur de contrôle cryptographique Sc_i vérifie la relation :

$$\vartheta_{KPM}(S_{KsMi})$$

On indique que cette opération de vérification consiste en une opération de vérification de signature, opération duale de l'opération de signature réalisée à l'étape 1006 pour obtenir la valeur de contrôle cryptographique Sc_i. Ainsi, à l'étape 1012, l'opération de vérification de signature est réalisée à partir de la clé publique mère KpM.

La mise en œuvre du procédé, objet de la présente invention, tel que décrit en liaison avec la figure 2a permet ainsi d'établir l'authenticité de la valeur de contrôle cryptographique précitée et en conséquence, notamment, l'origine de la requête de certification présentée à l'autorité de certification.

Dans des conditions qui seront explicitées ultérieurement dans la description, la vérification de cette requête, l'origine étant établie, permet , à partir de la valeur d'usage U précitée, de connaître de manière certaine le ou les usages dédiés qui peuvent être effectués avec la clé publique Kp, du fait des usages restrictifs sur les opérations pouvant être réalisés à l'aide de la clé privée Ks contenue dans le système embarqué. On peut alors émettre un certificat à même de garantir l'usage qui peut être fait de cette clé publique du fait des restrictions sur les opérations pouvant être réalisés à l'aide de la clé privée correspondante. Cette garantie d'usage pourra provenir de l'emploi combiné de deux informations qui seront alors présentes dans le certificat généré : d'une part l'indicateur d'usage de la clé publique et d'autre part un identifiant de politique de sécurité. Cette politique de sécurité pourra alors indiquer que la génération de clé a été faite sur un système embarqué réunissant les qualité requises pour limiter l'usage des clés privées générées sur cedit système embarqué. On pourra aussi utiliser toute autre champ d'extension du certificat

tel que cela est explicitement prévu par le standard X.509 v3.

Une variante de mise en œuvre du procédé, objet de la présente invention et permettant la vérification d'un gabarit de requête de certification GRCA, tel que décrit en figure 2a, sera maintenant donnée en relation avec la figure 2b. Dans les figures 2a et 2b, les mêmes étapes portent les mêmes références.

Ainsi qu'on pourra l'observer sur la figure 2b, suite à l'étape 1004 consistant à communiquer au système embarqué Si un gabarit de requête de certification GRCA mais préalablement à l'étape 1005 consistant à faire compléter par le système embarqué Si les champs manquants du gabarit de requête de certification GRCA, le procédé, objet de la présente invention, peut consister en outre à vérifier, en une étape 1004a, au niveau du système embarqué Si considéré, la syntaxe du gabarit de requête de certification précité afin de s'assurer qu'il s'agit bien d'une requête de certification. L'étape 1004a peut alors être suivie d'une étape 1004b consistant par exemple en une étape de test de la valeur vraie de cette vérification de syntaxe. A l'étape 1004a, la vérification de syntaxe est notée V(GRCA) et l'étape de test 1004b est notée V(GRCA)=vraie.

L'étape 1005 consistant à faire compléter par le système embarqué Si les champs manquants du gabarit de requête de certification GRCA peut alors être conditionnée à une vérification positive, c'est-à-dire à une réponse positive à l'étape de test 1004b précédemment mentionnée.

Au contraire, sur réponse négative à l'étape 1004b précitée, un retour 1004c à l'étape de chargement du gabarit de requête de certification GRCA à l'étape 1004 peut alors être prévu.

L'étape de vérification de syntaxe peut être conduite par une vérification de la syntaxe du gabarit de requête de certification GRCA, le processus de vérification précité pouvant dépendre de la structure du gabarit de requête de certification utilisée. Un exemple de processus de vérification de syntaxe sera donné ultérieurement dans la description.

Ainsi, le procédé objet de la présente invention permet, selon un premier aspect, de donner l'usage de la clé privée Ks à l'entité et en aucun cas de donner la connaissance de la valeur de cette clé privée à cette entité. Afin d'empêcher la connaissance de la valeur de la clé privée, le couple clé privée/clé publique est engendré par le système embarqué protégé et la clé privée est mise en œuvre par un algorithme situé directement dans le système embarqué. En aucun cas elle ne peut donc être connue à l'extérieur du système embarqué.

Selon un deuxième aspect remarquable du procédé objet de l'invention, afin de vérifier que la demande de certification d'une clé publique émane bien du système embarqué le procédé met en œuvre plusieurs techniques. En particulier il met en œuvre le calcul d'une somme de contrôle cryptographique qui permet de s'assurer que la requête émane bien d'un système embarqué personnalisé par l'opérateur OPj. L'état de l'art met déjà en œuvre certaines de ces techniques qui s'avèrent être peu souples d'emploi, comme il va être rappelé ci-dessous. Une première technique consiste à mettre dans chaque système embarqué une clé secrète à partir de laquelle sera effectué le calcul de la somme de contrôle cryptographique. L'inconvénient majeur de cette technique connue est de devoir communiquer à l'avance à chaque autorité de certification potentielle, et de manière confidentielle, la

valeur secrète de chaque système embarqué. Une première amélioration du dispositif consiste à utiliser un secret mère et à calculer le secret de chaque système embarqué à partir à la fois du numéro de série du système embarqué et du secret mère. L'inconvénient majeur, dans ce dernier cas, est de devoir communiquer à l'avance à chaque autorité de certification potentielle et de manière confidentielle la valeur secrète de chaque secret mère correspondant à un ensemble donné de systèmes embarqués.

Une originalité de l'invention est au contraire de ne communiquer au préalable aucune information confidentielle mais de rendre accessible à chaque autorité de certification potentielle que des informations publiques, à savoir: un identifiant d'opérateur habilité OP_j, une référence de l'ensemble Lk et bien entendu une valeur de la clé publique mère KpM associée à un indicateur de l'algorithme à mettre en œuvre CAlM.
Ces informations permettent alors à n'importe quelle autorité de certification de vérifier l'origine de la requête de n'importe quel système embarqué faisant partie d'un ensemble de systèmes embarqués.

Une description plus détaillée de la mise en œuvre de l'étape 1003 de calcul de chaque clé privée diversifiée KsM_i sera maintenant donnée en liaison avec la figure 3, le mode opératoire du calcul précité pouvant être mis en œuvre quel que soit le mode de réalisation du procédé, objet de l'invention, tel que décrit précédemment en liaison avec la figure 2a ou la figure 2b.

Le processus de diversification des clés mis en œuvre à l'étape 1003 tel que représenté en figure 3 peut ainsi consister en un processus supporté par un algorithme mis en œuvre sous le nom de Mécanisme de Signature à Apport Nul de Connaissance (*zero knowledge* en anglais) et des

algorithmes connus sous le nom de FIAT-SHAMIR ou GUILLOU-QUISQUATER utilisables à cette fin. Pour cette raison, ainsi qu'indiqué en figure 3, chaque clé privée diversifiée KsM_i est réputée obtenue par la mise en œuvre de processus supportés par les algorithmes de FIAT-SHAMIR F-S ou de GUILLOU-QUISQUATER G-Q et vérifie ainsi la relation :

$$KsM_i = D\text{-}F\text{-}S(KsM, SN_i)$$

$$KsM_i = D\text{-}G\text{-}Q(KsM, SN_i)$$

relation dans laquelle D-F-S et D-G-Q désignent la mise en œuvre des processus de diversification de clé supportés par les algorithmes de FIAT-SHAMIR et de GUILLOU-QUISQUATER respectivement.

La technique utilisée consiste à mettre dans chaque système embarqué une clé privée diversifiée calculée à partir du numéro de série du système embarqué et d'une clé privée mère, laquelle clé diversifiée servira au calcul de la somme de contrôle cryptographique. L'Autorité de Certification CA sera alors en mesure de vérifier l'exactitude de la somme de contrôle cryptographique ainsi calculée en mettant en œuvre l'algorithme CAlM correspondant au type d'algorithme utilisé et en utilisant uniquement le numéro de série du système embarqué et la clé publique mère correspondant à l'ensemble Lk dont fait partie le système embarqué.

De ce fait il n'est pas utile de connaître à l'avance quelle Autorité de Certification sera choisie par l'entité car chaque Autorité de Certification sera en mesure, et en particulier postérieurement à la réception de la requête de certificat, d'obtenir la clé publique mère correspondant à l'ensemble dont le système embarqué fait partie. La gestion d'un nombre important de systèmes embarqués, par exemple plusieurs millions, se trouve ainsi grandement simplifiée, permettant ainsi une large diffusion

de tels systèmes cryptographiques, en stricte conformité avec les dispositions législatives nationales en autorisant l'utilisation.

Différents éléments descriptifs de la structure de messages ou de données utilisés pour la mise en œuvre du procédé, objet de la présente invention, seront maintenant donnés en liaison avec les figures 4a à 4c.

Sur la figure 4a, on a représenté la structure d'un message de requête de certification dans une version simplifiée . Dans ce mode de réalisation simplifié, le système embarqué génère seul l'ensemble des champs de la requête RCA en concaténant les informations suivantes: le champ de clé publique qui comprend l'identifiant de l'algorithme utilisé CA1, la valeur de la clé publique Kp, et un champ d'usage de clé U, objets de la certification demandée. Ces champs peuvent, par exemple, faire l'objet d'un codage conforme au standard ASN1, pour *Abstract Syntax Notation 1* en vocable anglo-saxon, afin de pouvoir délimiter la taille de chaque champ et d'être sûr de la nature de chaque champ. Enfin, la valeur cryptographique de contrôle Sc_i, est calculée sur les informations précédentes puis ajoutée aux informations précédentes.

Dans ce mode de réalisation simplifié, l'ensemble des champs précité permet la mise en œuvre du procédé, objet de la présente invention, tel que représenté en figure 2a par exemple.

La figure 4b représente une structure de messages de requête complétée par exemple, au format conforme au codage ANS1 précité. Dans ce cas, le codage de ces messages est effectué selon le mode dit TLV où T désigne le type du champ, L la longueur de celui-ci et V la valeur du champ.

Sur la figure 4b, au point 1), on a représenté dans un tel cas la structure d'un gabarit de requête de

certification GRCA, lequel est réputé formé par une suite de champs TLV séquentiels ou imbriqués conformes au standard ASN1. Ce gabarit de requête est formé à l'extérieur du système embarqué. Il devra comporter, et cela est vérifié par le système embarqué, trois champs et seulement trois champs correspondant à : 1) un type de champ d'identifiant d'algorithme, 2) un type de champ de valeur de clé publique, 3) un type de champ d'un indicateur des usages de clé publique. L'emplacement de chacun de ces champs parmi les autres champs du gabarit de requête doit en outre correspondre à un emplacement bien précis, c'est à dire être précédé et suivi de différents types de champs prédéterminés.

Dans ces conditions, à partir du gabarit de requête de certification GRCA précité, la vérification de syntaxe représentée à l'étape 1004b de la figure 2b peut consister, à vérifier la valeur du type du premier champ, puis en fonction de ce type ou de la longueur de ce champ de passer au type suivant. Au passage il convient de mémoriser l'ensemble des divers types rencontrés puis de vérifier que les trois types de champs attendus sont situés aux endroits où ils doivent être placés. Pour chacun des trois champs, il convient ensuite de vérifier leur longueur et pour le champ CA1 sa valeur. En effet, il s'agit de vérifier que le type d'algorithme attendu correspond bien au type de clé généré et correspondant à cet algorithme. Pour les champs formés à l'extérieur du système embarqué qui devront contenir en définitive la valeur de la clé publique Kp et la valeur des indicateur d'usage de la clé U ces derniers peuvent contenir n'importe quelle valeur, les valeurs 0 ou 1 telles que représentées en figure 4b, puisque le système embarqué va leur substituer les valeurs adéquates et générées en interne.

Suite à la reconnaissance à la valeur vraie de la vérification ainsi effectuée, vérification notée V(GRCA) de l'étape 1004a de la figure 2b, les valeurs des deux champs peuvent être substituées par les valeurs générées par le système embarqué. Le champ d'usage U substitué peut consister en une chaîne de bits, le premier bit représentant par exemple un usage de chiffrement/déchiffrement C/D, la valeur 1 indiquant le chiffrement et la valeur 0 l'absence de chiffrement, le deuxième bit correspondant par exemple à un usage de signature numérique ou d'authentification A , le troisième bit correspondant par exemple à une opération de non-répudiation NR mettant en œuvre une signature numérique par exemple.

En ce qui concerne la valeur de la clé publique Kp, celle-ci peut être substituée à partir des valeurs de bit de cette clé correspondante.

Enfin, en référence à la figure 4c, la structure du gabarit de requête de certification GRCA, chargée à l'initiative de l'utilisateur Uti, peut comporter un champ relatif à un identifiant de cet utilisateur Uti, un champ relatif à la valeur de la clé Kp, clé publique dont la certification est demandée par ce dernier, un champ relatif à l'usage ou aux usages de cette clé U et un champ Plu relatif aux plages de validité ou d'utilisation de la clé Kp précitée.

De manière plus particulière, on indique que le champ relatif à l'identifiant de l'utilisateur Uti est rempli par l'utilisateur lors de sa demande de certification, alors que les champs relatifs à la valeur de la clé Kp et le champ relatif aux usages de cette clé sont remplis par le système embarqué lui-même.

En ce qui concerne le champ relatif à l'identifiant de l'utilisateur Uti, celui-ci peut correspondre au numéro de série SN_i du système embarqué lui-même.

Une description plus détaillée de la mise en œuvre de l'étape 1012 consistant pour l'autorité de certification à vérifier le message de requête de certification MRCA et en particulier la valeur de contrôle cryptographique Sc_i sera décrite en liaison avec la figure 5.

D'une manière générale, on indique que cette étape de vérification est effectuée grâce à un processus de vérification de signature, en particulier de vérification de la valeur de contrôle cryptographique Sc_i, laquelle n'est autre qu'une signature obtenue à partir de la clé privée diversifiée KsM_i à l'étape 1006 précédemment décrite dans la description. Dans ces conditions, l'opération de vérification ϑ_{KpM} consiste en l'opération duale de celle de celle réalisée à l'étape 1006 précitée.

Ainsi que représenté à la figure 5, les variables d'entrée, outre la clé publique mère KpM qui a été retrouvée suite à l'exécution des étapes 1009, 1010 et 1011 des figures 2a ou 2b, sont la valeur de contrôle cryptographique Sc_i et le message de requête de certification MRCA ainsi que l'identifiant IDd_i du système embarqué, c'est-à-dire l'identifiant de l'opérateur OP_j et le numéro de série SN_i du système embarqué considéré. L'opération de vérification précitée duale de l'opération de signature permet alors, à partir des variables entrées comme paramètres précédemment cités, une réponse par oui ou non, c'est-à-dire l'établissement de la valeur vraie ou de la valeur complémentée de cette valeur vraie, considérée comme valeur fausse, de l'opération de vérification.

Alors que l'origine de la requête de certification a pu ainsi être vérifiée conformément à la mise en œuvre du

procédé, objet de la présente invention, tel que représenté en figure 2a et/ou 2b, le procédé précité permet également de moduler la puissance des traitements cryptographiques, c'est-à-dire de chiffrement/ déchiffrement et calcul/vérification de signature, alloués à chaque système embarqué Si considéré.

Ainsi, conformément à un aspect particulièrement remarquable du procédé, objet de la présente invention, celui-ci permet, grâce à la certification demandée d'une clé publique donnée et des usages de cette clé publique, soit d'accréditer le système embarqué Si demandeur de cette certification pour réaliser des opérations de déchiffrement selon un processus supporté par un algorithme faible, ou encore de n'accréditer ce système embarqué ou l'entité titulaire de ce système embarqué que pour des opérations supportées par un algorithme limité à des opérations de calcul de signature seulement.

On comprend en particulier qu'en fonction de la valeur des bits de champ d'usage de la clé considérée, valeur d'usage codée par exemple sur 2 bits, la valeur 1X de ces 2 bits pouvant correspondre à un usage de déchiffrement selon un processus supporté par un algorithme faible, et la valeur X1 pouvant correspondre à une opération selon un processus supporté par un algorithme de génération de signature seulement, le système embarqué accrédité pourra réaliser l'une ou l'autre de ces opérations ou bien les deux opérations, mais pas d'autres opérations telles que le déchiffrement fort. Il est aussi précisé qu'un même système embarqué pourra comporter plusieurs clés, certaines comportant par exemple les bits d'usage avec la valeur 10 restreignant ainsi leur usage à des fins de déchiffrement faible et d'autres avec la valeur

01 restreignant ainsi leur usage à des fins de génération de signature.

Un processus de déchiffrement supporté par un algorithme faible, conformément à l'objet de la présente invention, sera maintenant décrit en liaison avec la figure 6.

De manière générale, on indique qu'une clé de chiffrement ou de déchiffrement utilisée par l'algorithme RSA, clé asymétrique, comprend en général 512 bits ou plus alors qu'une clé symétrique comporte généralement de 40 à 192 bits. Il est donc nécessaire de combler les bits restants, par exemple avec une entête. A titre d'exemple, il est possible, sur la chaîne de 512 bits ainsi créée, de prévoir une en-tête constituée par des valeurs spécifiques arbitraires fictives, les valeurs 02, 00 et en code hexadécimal FFF suivi de deux octets à la valeur 00 sur toute la valeur de l'en-tête auxquelles est concaténée une clé secrète symétrique, cadrée à droite, l'ensemble constituant une chaîne de bits de 512 bits. Dans le cas où la clé secrète symétrique KSF comporte 64 bits ou plus, le processus de déchiffrement à clé secrète symétrique est considéré comme fort et ne correspond pas à l'objet de la présente invention dans ce mode de réalisation.

Au contraire, lorsque le champ de clé secrète symétrique KSf est inférieur ou égal à 40 bits, le champ d'en-tête étant complété par exemple en conséquence par des valeurs hexadécimales FFF suivie d'un nombre prédéterminé de 00, le champ de clé secrète est un champ de clé secrète de déchiffrement symétrique faible et correspond ainsi à une fonction de déchiffrement faible susceptible d'être mise en œuvre conformément au procédé objet de la présente invention.

Dans un tel cas et conformément à un aspect particulièrement remarquable du procédé, objet de la présente invention, pour un jeu de clés asymétriques, clé publique de chiffrement notée Ep et clé privée de déchiffrement Ds engendrées par le système embarqué Si, la clé de chiffrement Ep correspondant à la clé publique Kp dont la certification est demandée ainsi que mentionné précédemment dans la description et la clé privée de déchiffrement Ds correspondant à la clé privée Ks mentionnée précédemment dans la description, le procédé objet de l'invention consiste alors à associer à la clé de déchiffrement Ds et au processus de déchiffrement asymétrique correspondant, supporté par exemple par l'algorithme RSA, un processus et une clé de déchiffrement faible supporté par exemple par l'algorithme DES et dont la clé symétrique est de longueur inférieure ou égale à 40 bits. Ainsi, en référence à la figure 6, on indique que la clé secrète symétrique faible, notée KSf, complétée de son en-tête de valeur arbitraire telle que mentionnée précédemment dans la description, est soumise à un processus de chiffrement pour obtenir une clé chiffrée à partir de la clé publique Ep de chiffrement asymétrique. La clé chiffrée ainsi obtenue est soumise ensuite à un processus de déchiffrement au moyen de la clé privée de déchiffrement asymétrique Ds alors que, conformément au procédé objet de la présente invention, cette clé privée de déchiffrement Ds est mémorisée dans la zone mémoire à accès externe protégé en écriture/lecture du système embarqué et est donc inconnue de l'utilisateur. Le processus de déchiffrement précité permet alors d'obtenir une clé déchiffrée dont la structure n'est autre que l'en-tête précédemment mentionnée dans la description et la clé symétrique faible KSf dont la longueur est déterminante.

Si la longueur de la clé symétrique faible KSf est inférieure ou égale à 40 bits, l'en-tête étant simplement discriminée par référence aux valeurs d'en-tête correspondantes et la clé symétrique et en particulier la clé symétrique faible KSf étant également discriminées en conséquence, cette clé symétrique faible KSf peut alors être mise à disposition de l'entité possédant le système embarqué pour des opérations de déchiffrement selon un processus supporté par un algorithme faible. Dans ces conditions, la clé symétrique de déchiffrement faible KSf permet à ce dernier de n'assurer que le déchiffrement de cryptogrammes C en messages M au moyen d'un algorithme de déchiffrement faible ainsi que représenté sur la figure 6.

Si au contraire, la longueur de la chaîne de bits représentative de la clé symétrique autre que l'en-tête précitée est supérieure à 40 bits la clé symétrique, dont la longueur est supérieure à 40 bits, n'est pas mise à disposition de l'entité possédant le système embarqué, laquelle n'est donc pas en mesure d' opérer des opérations de déchiffrement selon un processus supporté par un algorithme fort.

Un système embarqué permettant, notamment, la mise en œuvre du procédé objet de la présente invention sera maintenant décrit en liaison avec la figure 7. De manière non limitative, ce système embarqué est représenté et décrit sous la forme d'une carte à microprocesseur.

En référence à la figure 7 précitée, le système embarqué comprend, de manière classique, les mêmes éléments que ceux décrits en relation avec la figure 1, à savoir une unité de calcul 14, une mémoire vive 16, une mémoire non volatile 18 comportant une mémoire programmable 18a comprenant une zone mémoire à accès externe protégé MAP, un module de calcul cryptographique 20 et un système

d'entrée/sortie 12 reliés par une liaison de type BUS. Afin de permettre la mise en œuvre du procédé objet de la présente invention, ce système embarqué comporte au moins une clé diversifiée KsM_i mémorisée dans la mémoire MAP à accès externe protégé. Cette clé privée diversifiée est unique et distincte pour ce système embarqué. Elle est calculée à partir d'une clé privée mère KsM et d'un numéro d'identification de ce système embarqué et est associée à une clé publique mère KpM.

Le module cryptographique 20 comporte un module de calcul de signature MCS à partir de la clé privée diversifiée KsM_i, permettant de calculer la signature d'une requête de certification d'une clé publique Kp associée à une clé privée Ks de chiffrement, respectivement de signature. La clé privée Ks est engendrée par le module MCS de calcul de signature et mémorisée dans la mémoire à accès protégé MAP. La signature d'une requête de certification est fonction du numéro d'identification de ce système embarqué. Le module de calcul de signature MCS permet de transmettre à une autorité de certification un message de requête de certification comprenant cette requête de certification et la signature précitée. Ceci permet à l'autorité de certification de vérifier l'origine de la requête de certification de ce système embarqué 10 et la protection des clé privée diversifiée KsM_i et clé privée de signature Ks dans la mémoire à accès externe protégé MAP à partir de seuls éléments publics, tels que la clé publique mère KpM. En ce qui concerne le module de calcul de signature MCS, ce dernier peut être implanté dans une partie mémoire morte ROM 18b de la mémoire non volatile 18 et appelé sur requête par le module de calcul cryptographique 20.

REVENDICATIONS

1. Procédé de vérification de l'usage de clés publiques issues d'un jeu de clés asymétriques, clé publique (Kp) et clé privée (Ks) engendrées, pour un usage donné, tel que le chiffrement/déchiffrement ou la vérification/génération de signature numérique, par un système embarqué et mémorisées dans la zone mémoire d'un système embarqué (S_i) muni de moyens de calcul cryptographique et de moyens de mémorisation de données numériques à accès externe protégé en écriture/lecture, ces données numériques (IDd_i) comportant au moins un numéro de série (SN_i) permettant l'identification du système embarqué et un code d'identification (Op_j) d'un opérateur habilité à configurer ledit système embarqué et cette requête étant formulée par ledit système embarqué par transmission d'un message de requête (MRCA) contenant ladite clé publique (Kp) à une autorité de certification (CA), caractérisé en ce que ce procédé consiste :

• préalablement à toute transmission d'une requête de certification, lors de la configuration de ces systèmes embarqués par cet opérateur habilité pour tous les systèmes embarqués (S_i) d'un ensemble (Lk) de systèmes embarqués :

- à faire engendrer par cet opérateur habilité, pour cet ensemble donné de systèmes embarqués, une clé publique mère (KpM) et une clé privée mère (KsM) mis en œuvre dans le cadre d'un processus supporté par un algorithme (CAlM) ;
- à publier ladite clé publique mère (KpM) associée à l'algorithme (CAlM), l'identité de cet opérateur habilité (OP_j) et à un ensemble (Lk) définissant une plage d'identifiants de systèmes embarqués ;
- à calculer, pour chaque système embarqué appartenant à cet ensemble (Lk) de systèmes embarqués, à partir de

ladite clé privée mère (KsM) et du numéro de série (SN_i) du système embarqué, une clé privée diversifiée (KsM_i) et à mémoriser, dans ladite zone mémoire à accès externe protégé en écriture/lecture, ladite clé privée diversifiée (KsM_i), et

• préalablement à toute transmission d'un message de requête de certification :

- à faire engendrer par l'intermédiaire du système embarqué une requête de certification (RCA), contenant en particulier un champ de la clé publique (CAl,Kp) et les indicateurs d'usage (U) de cette clé publique,
- à calculer, au moyen desdits moyens de calcul et de ladite clé diversifiée (KsMi) associée à ce système embarqué, une valeur de contrôle cryptographique (Sc_i) sur l'ensemble de la requête (RCA), ladite valeur de contrôle cryptographique étant une signature numérique calculée au moyen de la clé privée diversifiée (KsM_i);

• lors de l'émission, par le système embarqué, d'une requête de certification à l'autorité de certification :

- à former un message de requête de certification (MRCA) contenant la requête (RCA), l'identifiant (IDd_i) du système embarqué, ce dernier étant constitué d'une part de l'identifiant (OP_j) de cet opérateur habilité et d'autre part du numéro de série (SN_i) du système embarqué, et la valeur de contrôle cryptographique (Sc_i)
- à transmettre à l'autorité de certification (CA) ledit message de requête (MRCA) formé lors de la phase précédente et contenant la clé publique (Kp) et les indicateurs d'usage (U), objets de ladite certification, et ladite valeur de contrôle cryptographique (Sc_i) ;

• lors de la réception d'un message de requête de certification (MRCA) par l'autorité de certification :

- à retrouver, l'identité de l'opérateur habilité (OP_j) à partir de l'identifiant (IDd_i) du système embarqué,
- à retrouver, à partir dudit identifiant (OP_J) de cet opérateur habilité la valeur de la clé publique mère (KpM) ainsi que l'identifiant de l'algorithme (CAlM) associé à l'ensemble auquel appartient le système embarqué,
- à vérifier à partir de ladite clé publique mère (KpM), dudit numéro de série (SN_i) du système embarqué, dudit message de requête de certification reçu (MRCA), ladite valeur de contrôle cryptographique (Sc_i), ce qui permet d'établir l'authenticité de cette valeur de contrôle cryptographique et l'origine de cette requête de certification.

2. Procédé selon la revendication 1, caractérisé en ce que, lorsque la requête de certification est engendrée par le système embarqué, celui-ci consiste en outre :

- à générer, au niveau du système embarqué, la requête de certification (RCA), laquelle est alors composée de trois champs à savoir: un identifiant d'algorithme à clé publique (CAl), une valeur de clé publique (Kp), et un indicateur des usages de cette clé (U).

3. Procédé selon la revendication 1, caractérisé en ce que, lorsque la requête de certification est complétée par le système embarqué lors de l'étape consistant à communiquer audit système embarqué un gabarit de requête de certification (GRCA), celui-ci consiste en outre :

- à vérifier, au niveau du système embarqué, la syntaxe du gabarit de requête de certification (GRCA) afin de s'assurer qu'il s'agit d'une requête de certification bien formée, et
- à conditionner à une vérification positive, l'étape consistant à faire compléter par le système embarqué les

champs manquants du gabarit de requête de certification (GRCA).

4. Procédé selon la revendication 1, caractérisé en ce que, pour un jeu de clés asymétriques de signature (Kp), (Ks) engendrées par ledit système embarqué, les moyens de calcul cryptographique de ce système embarqué, n'autorisant d'utiliser la clé privée (Ks) qu'à des fins de génération de signature, ladite clé privée (Ks) mémorisée dans ladite zone mémoire à accès externe protégé en écriture/lecture étant inconnue de l'utilisateur et restreinte d'utilisation à des fins exclusives de signature numérique, l'utilisation de ladite clé est restreinte à des fins de signature et l'utilisation du certificat contenant la clé publique correspondante est limitée en pratique à des fins de vérification de signature.

5. Procédé selon la revendication 1, caractérisé en ce que, pour un jeu de clés asymétriques clé publique de chiffrement (Ep) et clé privée de déchiffrement (Ds) engendrées par ledit système embarqué, celui-ci consiste à associer auxdites clés (Ep), (Ds) et processus de déchiffrement asymétrique un processus et une clé de déchiffrement symétrique "faible", la clé symétrique de déchiffrement étant chiffrée puis déchiffrée au moyen de la clé privée de déchiffrement asymétrique (Ds), ladite clé privée (Ds) mémorisée dans ladite zone mémoire à accès externe protégé en écriture/lecture étant inconnue de l'utilisateur, ce qui permet de n'autoriser l'utilisation de ladite clé qu'à des fins de déchiffrement faible et l'utilisation du certificat contenant la clé publique correspondante étant limitée en pratique à des fins de chiffrement faible.

6. Système embarqué comprenant une unité de calcul, une mémoire vive, une mémoire non volatile comportant une

mémoire programmable comprenant une zone mémoire à accès externe protégé, un module de calcul cryptographique et un système d'entrée/sortie reliés par une liaison de type BUS, caractérisé en ce que ledit système embarqué comporte au moins :

- une clé diversifiée KsM_i mémorisée dans ladite mémoire à accès externe protégé, ladite clé privée diversifiée unique et distincte pour ce système embarqué calculée à partir d'une clé privée mère KsM et d'un numéro d'identification de ce système embarqué étant associée à une clé publique mère KpM ; ledit module de calcul cryptographique comportant

- des moyens de calcul de signature, à partir de ladite clé privée diversifiée KsM_i, permettant de calculer la signature d'une requête de certification d'une clé publique Kp associée à une clé privée Ks de chiffrement, respectivement de signature, ladite clé privée Ks engendrée par lesdits moyens de calcul de signature étant mémorisée dans ladite mémoire à accès protégé, cette signature d'une requête de certification étant fonction du numéro d'identification de ce système embarqué, lesdits moyens de calcul de signature permettant de transmettre à une autorité de certification un message de requête de certification contenant ladite requête de certification et ladite signature, ce qui permet à ladite autorité de certification de vérifier l'origine de la requête de certification de ce système embarqué et la protection desdites clé privée diversifiée et clé privée de signature dans ladite mémoire à accès externe protégé à partir de seuls éléments publics, tels que ladite clé publique mère KpM.

ABREGE DESCRIPTIF

Un procédé et un système embarqué de vérification d'une requête de certification de clé publique (Kp) engendrée par un système embarqué d'identifiant (SN_i).

Pour un ensemble (Lk) de systèmes embarqués, un opérateur habilité d'identifiant (OP_j) configure les systèmes embarqués et crée (1001) une clé publique mère (KpM) et une clé privée mère (KsM). L'identifiant (Op_j), la plage d'identifiants référencée (Lk) et la clé publique mère (KpM) sont publiés (1002). Pour chaque système embarqué (SN_i), une clé diversifiée (KsM_i) est créée à partir de l'identifiant (SN_i) et mémorisée (1003) en mémoire à accès protégé en lecture et écriture. Pour toute clé publique (Kp) engendrée par un système embarqué, une valeur de contrôle cryptographique (Sci) est calculée (1006) sur la clé publique (Kp), un identifiant d'algorithme (CAl) et des paramètres d'utilisation (U) de cette clé à l'aide d'un algorithme de signature à apport nul de connaissance et un message de requête de certification (MRCA) comprenant la valeur de contrôle (Sci), l'identifiant de l'opérateur (Op_j) et l'identifiant (SN_i) est transmis à une autorité de certification, laquelle retrouve l'identifiant (Op_j) (1009) et la valeur de la clé publique mère (KpM) (1011). Une vérification (1012) du message (MRCA) à partir de la clé publique mère (KpM) et de l'identifiant du système embarqué (SN_i) permet de s'assurer que la requête de certification de clé publique (Kp) et l'utilisation de celle-ci provient bien d'un composant embarqué à même de limiter l'utilisation de cette clé.

Figure 2a.

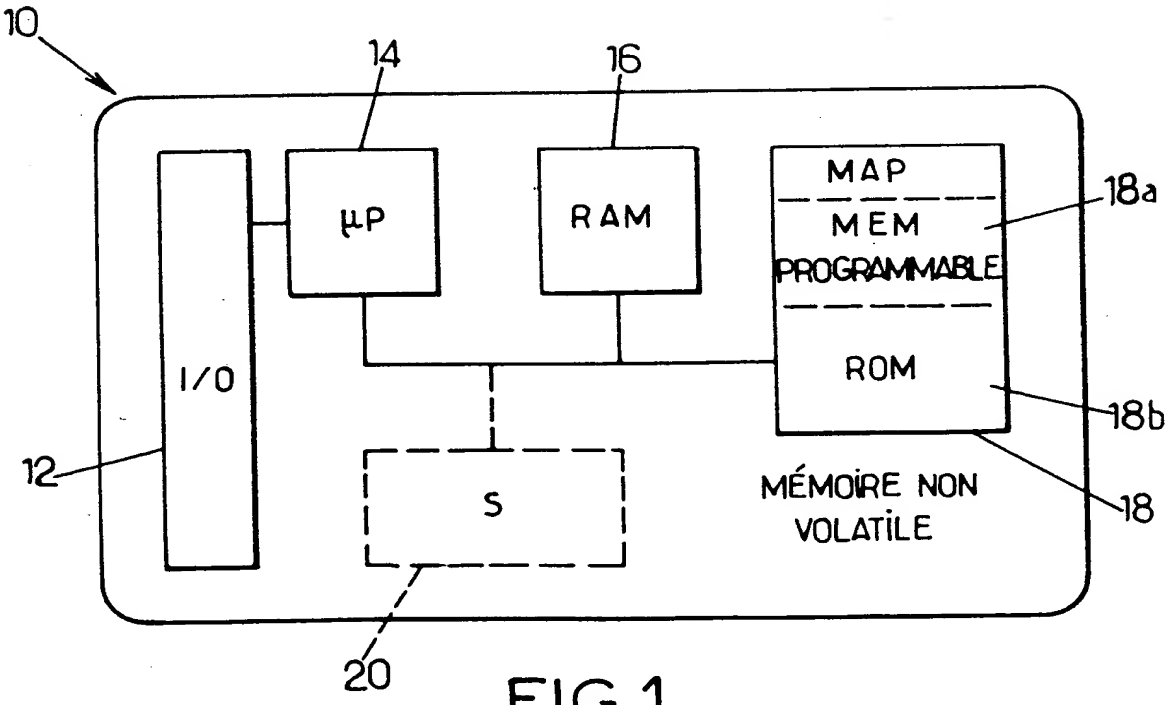


FIG.1.
(ART ANTÉRIEUR)

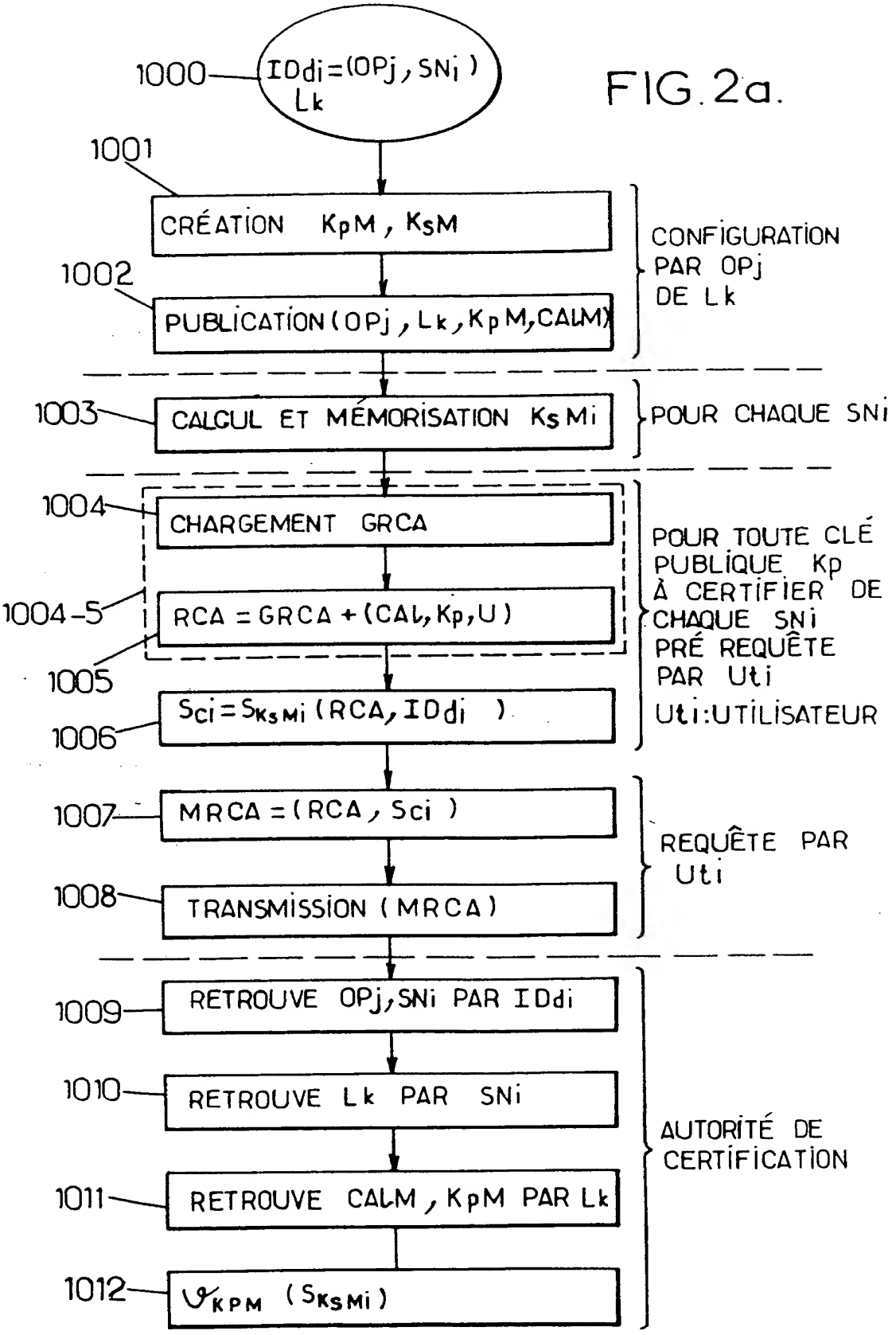

1000
IDdi=(OPj, SNi)
Lk
1001
CRÉATION KpM, KsM
1002
PUBLICATION (OPj, Lk, KpM, CALM)
CONFIGURATION PAR OPj DE Lk
1003
CALCUL ET MÉMORISATION KsMi
POUR CHAQUE SNi
1004
CHARGEMENT GRCA
1004-5
RCA = GRCA + (CAL, Kp, U)
1005
Sci = SksMi (RCA, IDdi)
1006
POUR TOUTE CLÉ PUBLIQUE Kp À CERTIFIER DE CHAQUE SNi PRÉ REQUÊTE PAR Uti
Uti: UTILISATEUR
1007
MRCA = (RCA, Sci)
1008
TRANSMISSION (MRCA)
REQUÊTE PAR Uti
1009
RETROUVE OPj, SNi PAR IDdi
1010
RETROUVE Lk PAR SNi
1011
RETROUVE CALM, KpM PAR Lk
1012
ψKPM (SksMi)
AUTORITÉ DE CERTIFICATION

FIG. 2a.

FIG.2b.

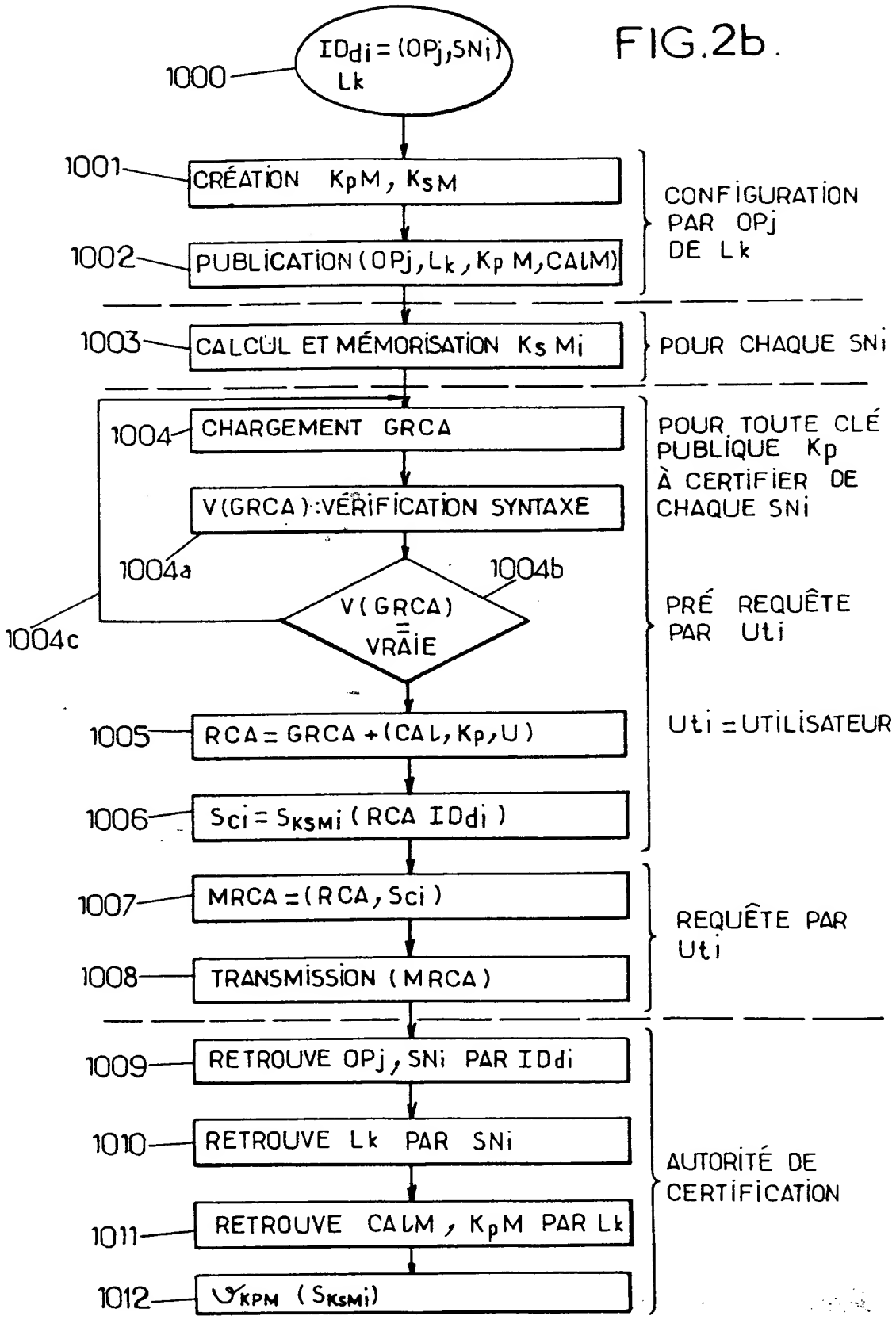

1000
IDdi = (OPj, SNi) Lk
1001
CRÉATION KpM, KsM
1002
PUBLICATION (OPj, Lk, Kp M, CALM)
CONFIGURATION PAR OPj DE Lk
1003
CALCUL ET MÉMORISATION Ks Mi
POUR CHAQUE SNi
1004
CHARGEMENT GRCA
V(GRCA):VÉRIFICATION SYNTAXE
1004a
1004b
V(GRCA) VRAIE
1004c
POUR TOUTE CLÉ PUBLIQUE Kp À CERTIFIER DE CHAQUE SNi
PRÉ REQUÊTE PAR Uti
Uti = UTILISATEUR
1005
RCA = GRCA + (CAL, Kp, U)
1006
Sci = SKSMi (RCA IDdi)
1007
MRCA = (RCA, Sci)
1008
TRANSMISSION (MRCA)
REQUÊTE PAR Uti
1009
RETROUVE OPj, SNi PAR IDdi
1010
RETROUVE Lk PAR SNi
1011
RETROUVE CALM, KpM PAR Lk
1012
SKPM (SKSMi)
AUTORITÉ DE CERTIFICATION

FIG.3.

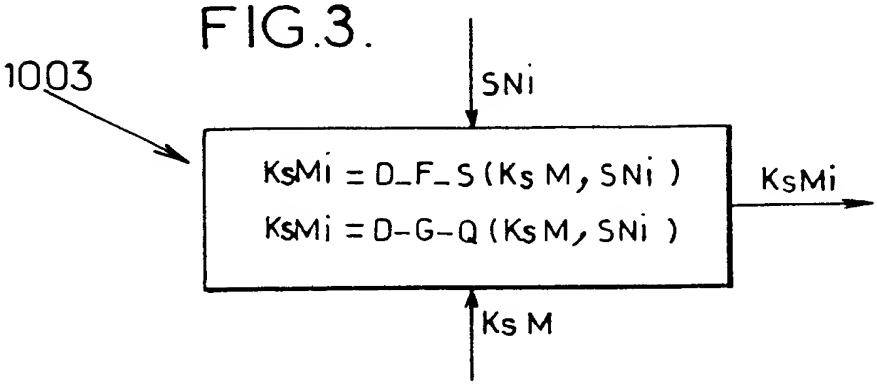


FIG.5.

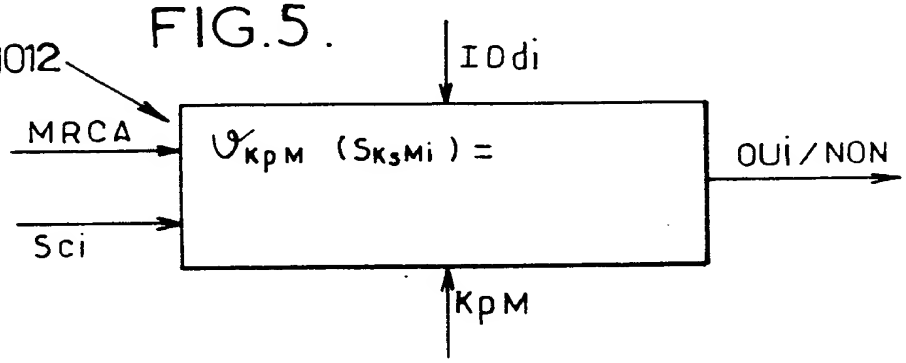


FIG.6.

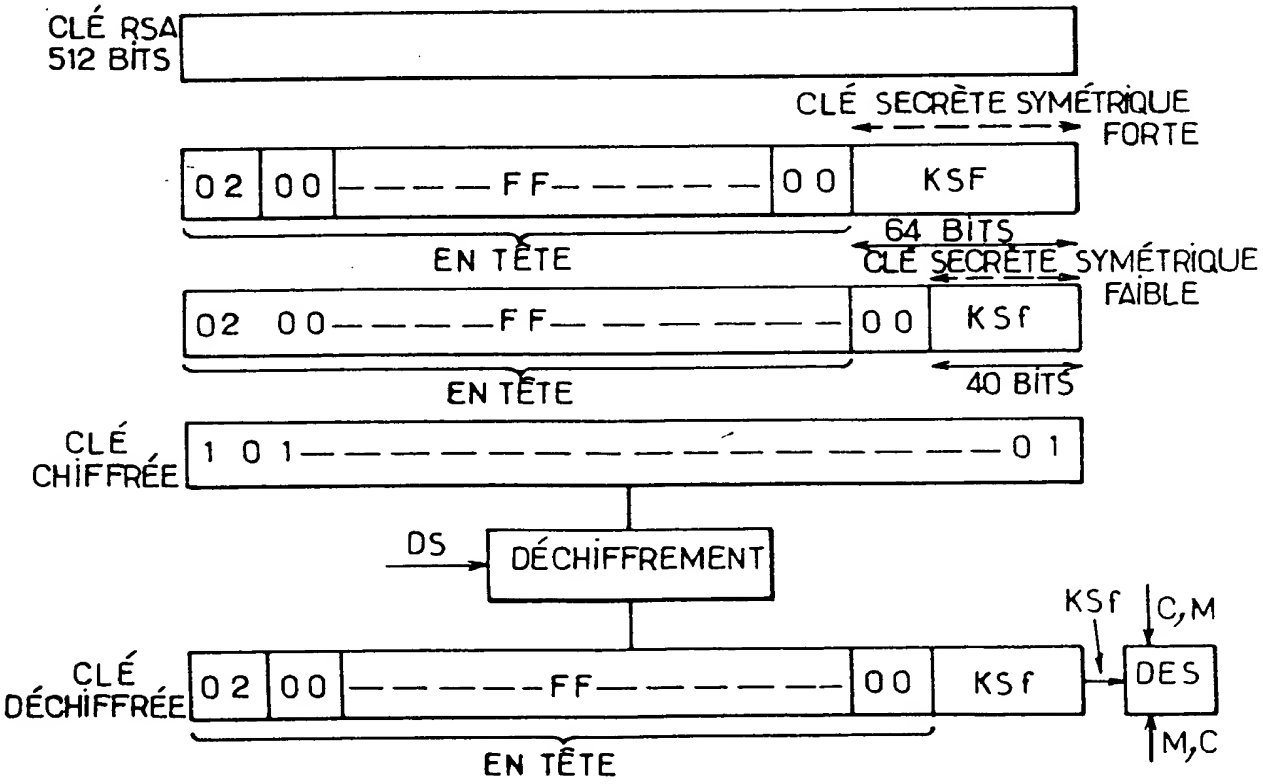


FIG.4a.

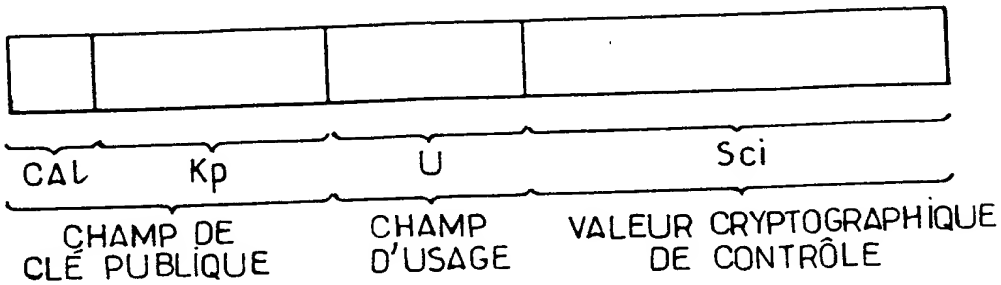


FIG.4b.

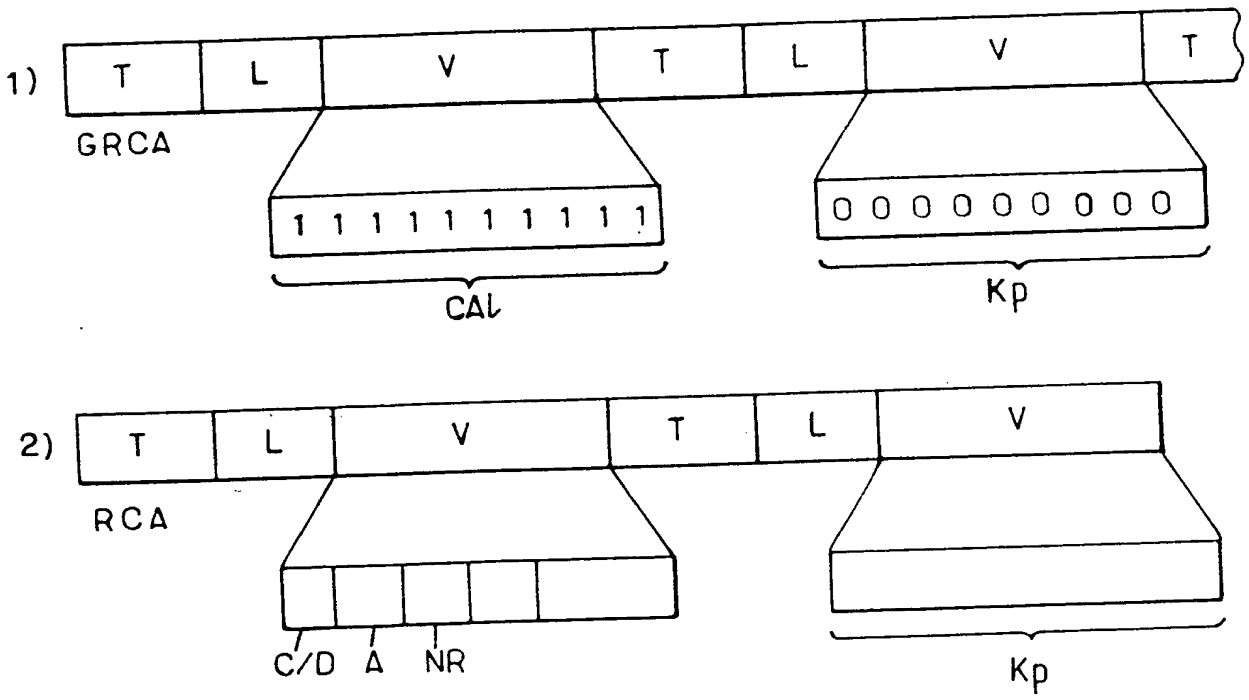
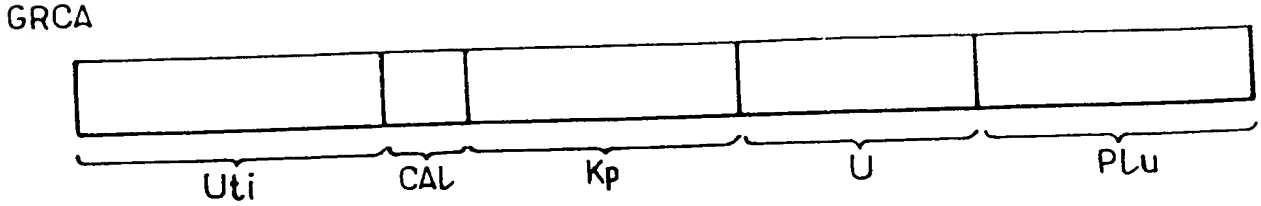


FIG.4c.



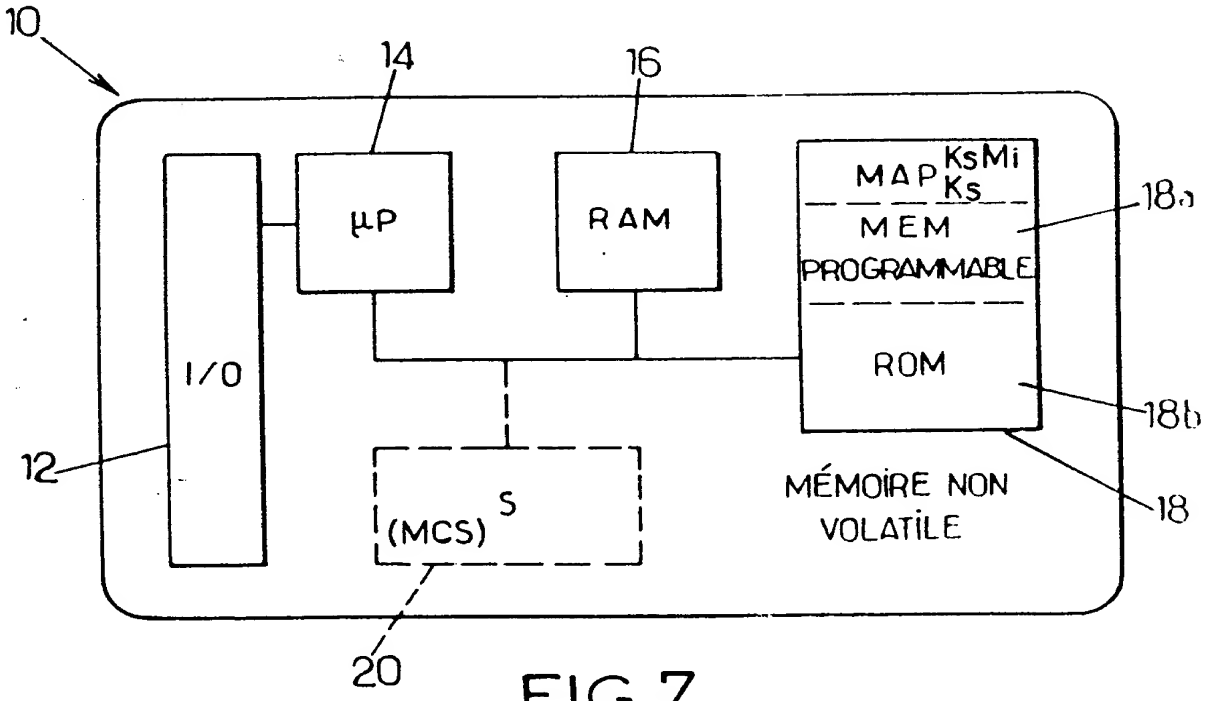

10
14
16
µP
RAM
MAP KsMi Ks
MEM PROGRAMMABLE
18a
I/O
ROM
18b
12
(MCS) S
MÉMOIRE NON VOLATILE
18
20

FIG.7.